

\* Day: Tuesday  
\* Subject: Abstract algebra (3)

\* Date: 17/12/2015  
\* Lecture: 1

## (1) Ideals:

### I. Definition:

(1) Let  $R$  be a ring and  $I$  be a nonempty subset of  $R$ , then:

( $\alpha$ )  $I$  is called a left ideal of  $R$  if:

(i)  $a - b \in I \quad \forall a, b \in I$ .

(ii)  $ra \in I \quad \forall a \in I, r \in R$

( $\beta$ )  $I$  is called a right ideal of  $R$  if:

(i)  $a - b \in I \quad \forall a, b \in I$ .

(ii)  $ar \in I \quad \forall a \in I, r \in R$ .

( $\gamma$ )  $I$  is called an ideal of  $R$  if:

(i)  $a - b \in I \quad \forall a, b \in I$ .

(ii)  $ra \in I \quad \forall a \in I, r \in R$ .

(iii)  $ar \in I \quad \forall a \in I, r \in R$ .

(2) Let  $R$  be a ring and  $I$  be a nonempty subset of  $R$ , then  $I$  is called an ideal of  $R$ , denoted by  $I \triangleleft R$ , if:

(i)  $a - b \in I \quad \forall a, b \in I$ .

(ii)  $rI \subseteq I \quad \forall r \in R$ .

(iii)  $Ir \subseteq I \quad \forall r \in R$ .

(3) A nonempty subset  $I$  of a ring  $R$  is an ideal of  $R$  (i.e.  $I \triangleleft R$ ) if and only if:

(i)  $(I, +)$  is a subgroup of  $(R, +)$ .

(ii)  $ra \in I \quad \forall a \in I, r \in R$ .



$$(iii) ar \in I \quad \forall a \in I, r \in R.$$

## II. Remark:

(1) If  $I$  is an ideal of  $R$  (right or left), then  $I$  is a subring of  $R$ .

$$\text{i.e. } I \triangleleft R \Rightarrow I \leq R \Rightarrow I \subseteq R$$

(2) If  $R$  is a commutative ring, then every left ideal of  $R$  is also a right ideal and every right ideal is also a left ideal of  $R$ .

(3) For commutative rings, every left or right ideal is an ideal.

(4) If  $R$  is a ring, then the subsets  $\{0\}, R$  of  $R$  are ideals of  $R$  and these ideals are called trivial ideals. All other ideals are called non-trivial.

(5) An ideal  $I$  of a ring  $R$  is called a proper ideal of  $R$  if  $\{0\} \neq I \neq R$ .

(6) The sets  $rI$  and  $Ir$  are:

$$rI = \{ra : a \in I, r \in R\}$$

$$Ir = \{ar : a \in I, r \in R\}$$

## III. Example:

Let  $n \in \mathbb{Z}$ ,  $I = \{nk : k \in \mathbb{Z}\}$ , then  $I \triangleleft \mathbb{Z}$ .

Let  $nk_1, nk_2 \in I$

$$nk_1 - nk_2 = n(k_1 - k_2) \in I \quad \rightarrow (i)$$

Let  $nk \in I$  and  $r \in \mathbb{Z}$

$$r(nk) = rnk = (rn)k = (nr)k = n(rk) \in \mathbb{Z} \rightarrow (ii)$$

$$(nk)r = nkr = n(kr) \in I \quad \rightarrow (iii)$$

from (i), (ii) and (iii) then  $I \triangleleft \mathbb{Z}$ .



## (2) Quotient (factor) rings:

### I. Definition:

- (1) Let  $R$  be a ring and  $I$  be an ideal of  $R$ .  
Let  $R/I$  denote the set:

$$R/I = \{x+I \mid x \in R\}$$

Define the operations  $+$  and  $\cdot$  on  $R/I$  as:

$$(i) (x+I) + (y+I) = (x+y) + I$$

$$\forall (x+I), (y+I) \in R/I.$$

$$(ii) (x+I) \cdot (y+I) = (x \cdot y) + I$$

$$\forall (x+I), (y+I) \in R/I.$$

under these binary operations, the system  
 $(R/I, +, \cdot)$  constitutes a ring.

- (2) If  $R$  is a ring and  $I$  is an ideal of  $R$ , then the ring  $(R/I, +, \cdot)$  is called the quotient (factor) ring of  $R$  by  $I$ .

### II. Remark:

- (1) The set  $x+I$  is defined as:

$$x+I = \{x+a \mid a \in I, x \in R\} = \{x+a_1, x+a_2, \dots\}$$

- (2) If  $R$  is commutative, then  $R/I$  is commutative.

- (3) If  $R$  has a unity  $(1)$ , then  $R/I$  has a unity  $(1+I)$ .

## (3) principal ideal domain: (P.I.D)

### I. Definition: (principal ideal)

If  $R$  is a commutative ring with unity and  $a \in R$ , then the ideal  $\{ra \mid r \in R\}$  of all multiples of  $a$  is the principal ideal generated by  $a$  and is denoted by  $\langle a \rangle$ .

→ An ideal  $I$  of  $R$  is a principal ideal if  $I = \langle a \rangle$  for some  $a \in R$ .



## II. Definition : (principal ideal domain)

An integral domain  $D$  is a principal ideal domain (abbreviated PID) if every ideal in  $D$  is a principal ideal.

## III. Example :

$\mathbb{Z}$  (The set of integers) is a principal ideal domain  
\* proof = (Later)

## (4) Prime and maximal ideals :

### I. Theorem :

If  $R$  is a ring with unity and  $N$  is an ideal of  $R$  containing a unit, then  $N = R$ .

■ proof :

Let  $R$  be a ring with unity and  $N$  is an ideal of  $R$ . Suppose that  $u \in N$ , where  $u$  is a unit in  $R$ .

$$\therefore N \triangleleft R$$

$$\therefore ru \in N \quad \forall r \in R, u \in N.$$

By taking  $r = u^{-1} \in R$

$$\Rightarrow u^{-1}u \in N \quad \text{but } uu^{-1} = 1 \Rightarrow 1 \in N$$

$$\therefore ru \in N \quad \forall r \in R, u \in N, \therefore 1 \in N$$

$$\therefore r \cdot 1 \in N \quad \forall r \in R \Rightarrow r \in N \quad \forall r \in R$$

$$\therefore R \subset N \rightarrow (i)$$

$$\therefore N \triangleleft R \quad \therefore N \subseteq R \rightarrow (ii)$$

From (i) and (ii), then  $N = R$  #

### II. Corollary :

A field contains no proper nontrivial ideals.

■ proof :

Let  $F$  be a field and  $\{0\} \neq N \triangleleft F$

Since every nonzero element of a field is a unit.



Hence,  $\exists u \in N, u^{-1} \in F \ni u^{-1}u \in N \Rightarrow 1 \in N$ .

$\therefore N \triangleleft F \Rightarrow \forall u \in N \forall r \in F, u \in N$ .

$\therefore 1 \in N \Rightarrow$  put  $u=1 \Rightarrow r \cdot 1 \in N \forall r \in F$   
 $\Rightarrow r \in N \forall r \in F$

$\therefore F \subseteq N \rightarrow (i)$

$\therefore N \triangleleft F \Rightarrow N \subseteq F \rightarrow (ii)$

from (i) and (ii)  $\Rightarrow N = F$ . #

### III. Maximal ideal:

A maximal ideal of a ring  $R$  is an ideal  $M$  different from  $R$  such that there is no proper ideal  $N$  of  $R$  properly containing  $M$ .

i.e.  $M \triangleleft R$ ,  $M$  is maximal  $\Rightarrow \nexists N \triangleleft R \ni M \subset N$   
or  $M \triangleleft R, N \triangleleft R, M \subset N \subset R \Rightarrow M = N$  or  $N = R$ .

➤ Example:

$2\mathbb{Z}$  is a maximal ideal of  $\mathbb{Z}$ , where  $2\mathbb{Z} \subseteq \mathbb{Z}$ ,  
 $4\mathbb{Z} \subseteq 2\mathbb{Z}$ .

$$\mathbb{Z} = \{ \dots, -2, -1, 0, 1, 2, \dots \}$$

$$2\mathbb{Z} = \{ \dots, -4, -2, 0, 2, 4, \dots \}$$

$$4\mathbb{Z} = \{ \dots, -8, -4, 0, 4, 8, \dots \}$$

### IV. prime ideal:

An ideal  $N \neq R$  in a commutative ring  $R$  is a prime ideal if  $ab \in N$  implies that either  $a \in N$  or  $b \in N$  for  $a, b \in R$ .

i.e.  $N$  prime ideal  $\Leftrightarrow (ab \in N \Rightarrow a \in N \text{ or } b \in N)$

➤ Example:

(1)  $N = \{0\}$  is a prime ideal in  $\mathbb{Z}$ .

(2)  $2\mathbb{Z} = \{ \dots, -4, -2, 0, 2, 4, \dots \}$  is a prime ideal of  $\mathbb{Z}$ .

(3)  $4\mathbb{Z} = \{ \dots, -8, -4, 0, 4, 8, \dots \}$  isn't a prime



ideal of  $\mathbb{Z}$ , because  $4 = 2 \cdot 2$  and  $2 \notin 4\mathbb{Z}$

(4)  $5\mathbb{Z} = \{ \dots, -10, -5, 0, 5, 10, \dots \}$  is a prime ideal of  $\mathbb{Z}$

◆ Remark:

(1) In  $\mathbb{Z}$ , the ideals  $N = \{0\}$  and  $N = p\mathbb{Z}$  where  $p$  is a prime number are prime ideals.

(2) For a commutative ring with unity, every maximal ideal is a prime ideal but not always vice versa.

(3) In  $\mathbb{Z}$ ,  $\{0\}$  is a prime ideal but not a maximal ideal.

(4) In case of  $\mathbb{R}$  without unity, then  $\exists$  maximal ideal but  $\nexists$  prime ideal.

for example;  $\mathbb{R} = 2\mathbb{Z}$ ,  $\langle 4 \rangle \subset 2\mathbb{Z} \Rightarrow$

$\langle 4 \rangle$  is a maximal ideal but not a prime ideal.

(5) Theorems:

For a commutative ring with unity:

(1) An ideal  $M$  of  $\mathbb{R}$  is maximal if and only if  $\mathbb{R}/M$  is a field.

(2) An ideal  $N$  of  $\mathbb{R}$  is prime if and only if  $\mathbb{R}/N$  is an integral domain.

(3) Every maximal ideal of  $\mathbb{R}$  is a prime ideal.

■ proof: (of number (3)).

Let  $\mathbb{R}$  be an Abelian ring with unity and  $M$  be a maximal ideal of  $\mathbb{R}$ .

using theorem (1)  $\Rightarrow \mathbb{R}/M$  is a field.

Since every field is an integral domain.

Hence,  $\mathbb{R}/M$  is an integral domain.

using theorem (2)  $\Rightarrow M$  is a prime ideal of  $\mathbb{R}$ .



$\mathbb{K}$  is a principal ideal domain.

proof:

we know that  $\mathbb{K}$  is an integral domain.

Then to prove that  $\mathbb{K}$  is a principal ideal domain, all we need to do is to prove that every ideal in  $\mathbb{K}$  is a principal ideal.

Let  $n \in \mathbb{K}$ ,  $N \triangleleft \mathbb{K} \Rightarrow N = \langle n \rangle$ .

(1) at  $n=0 \Rightarrow N = \{0\} = \langle 0 \rangle \Rightarrow N$  is principal ideal.

(2) at  $n=1 \Rightarrow N = \mathbb{K} = \langle 1 \rangle \Rightarrow N$  is principal ideal.

(3) at  $n \neq 0$  and  $n \neq 1$  i.e.  $\{0\} \neq N \neq \mathbb{K}$ .

we need to prove that  $N = \langle n \rangle$  where  $n$  is the smallest integer in  $N$ .

Let  $m \in N$ ,  $m > n$ .

using division algorithm in  $\mathbb{K}$ .

$\Rightarrow \exists a, r \in \mathbb{K} \exists m = na + r$ ,  $0 \leq r < n$ .

$\Rightarrow r = m - na$ .

$\because m \in N$  and  $n \in N \Rightarrow na \in N$  and  $m - na \in N$ .

$\therefore r = m - na \in N$ .

which is contradiction to the assumption that  $n$  is the smallest integer in  $N$  because we have  $r < n$ .

$\therefore r = 0$ .

$\Rightarrow 0 = m - na \Rightarrow m = na$  if  $m > n$ .

$\therefore N = \langle n \rangle \Rightarrow N$  is a principal ideal.

$\therefore \mathbb{K}$  is a principal ideal domain.



\* Day: Tuesday

\* Subject: Abstract algebra (3)

\* Date: 24/2/2015

\* Lecture: 2

### (1) Theorem:

For a commutative ring with unity  $R$ :

(I) An ideal  $M$  of  $R$  is maximal if and only if  $R/M$  is a field.

(II) An ideal  $I$  of  $R$  is prime if and only if  $R/I$  is an integral domain.

(III) Every maximal ideal of  $R$  is a prime ideal.

■ proof:

(I)  $M \triangleleft R$ ,  $M$  is maximal  $\iff R/M$  is a field.

(i) proving that:

$M \triangleleft R$ ,  $M$  is maximal  $\implies R/M$  is a field.

Let  $M$  be a maximal ideal of  $R$ .

$\therefore R$  is a commutative ring with unity ( $1$ ).

$\therefore R/M$  is a commutative ring with unity ( $1+M$ ).

To prove that  $R/M$  is a field, then we only need to prove that every nonzero element of  $R/M$  is a unit.  
i.e.  $\forall \bar{a} \neq \bar{0} \exists \bar{b} \neq \bar{0} \in R/M \ni \bar{a}\bar{b} = 1+M = \bar{1}$ .

Let  $\bar{0} \neq \bar{b} \in R/M$ ,  $\bar{b} = b+M \neq M$

$\implies b \notin M$  (i.e.  $b \in R$ ,  $b \notin M$ ).

Define  $Rb = \{rb \mid r \in R\}$ ; Hence we need to prove that  $Rb$  is an ideal of  $R$  (i.e.  $Rb \triangleleft R$ )

Let  $r_1b, r_2b \in Rb$

$\implies r_1b - r_2b = (r_1 - r_2)b \in Rb \rightarrow (1)$

$\therefore R$  is a commutative ring.



why?  $\Rightarrow MCM + Rb$

Because:

$$b \in B, B \subseteq R \Rightarrow b \in R$$

$$M + Rb = \{m + rb \mid r, b \in R, m \in M\}$$

Since  $R$  is a ring, then  $0 \in R$ .

Put  $r=0$

$$\therefore M + Rb = \{m + 0b \mid r, b \in R, m \in M\}$$

$$\Rightarrow M + Rb = \{m \mid m \in M\} = M$$

$\therefore M + Rb = M$  at  $r=0$ . (and this is a special case (I))

I mean that  $r$  can take other values different from 0

$$\therefore MCM + Rb$$



$$\therefore Rb = bR \rightarrow (2)$$

- from (1) and (2)  $\Rightarrow Rb \triangleleft R$ .

$$\therefore M \triangleleft R \text{ and } Rb \triangleleft R$$

$$\therefore M + Rb \triangleleft R \text{ (theorem)}$$

$$\therefore M \subseteq M + Rb, \overset{\text{why?!}}{M + Rb} \subseteq R$$

$$\therefore M \subseteq M + Rb \subseteq R$$

$\therefore M$  is a maximal ideal of  $R$ .

$$\therefore M + Rb = R$$

$$\therefore 1 \in R \quad \therefore 1 \in M + Rb$$

$$\therefore \exists a \in R \text{ s.t. } ab + M = 1 + M$$

$$\Rightarrow (a + M) \cdot (b + M) = 1 + M$$

Now, for each  $\bar{b} \neq \bar{0} \in R/M$ , there exists  $\bar{a} \neq \bar{0} \in R/M$  such that  $\bar{a}\bar{b} = \bar{1}$  i.e.  $(a + M) \cdot (b + M) = 1 + M$ .

Hence, each nonzero element of  $R/M$  has a multiplicative inverse.

$\therefore R/M$  is a field.

(ii) proving that:

$R/M$  is a field  $\Rightarrow M$  is maximal ideal of  $R$ .

Let  $B$  be an ideal of  $R$  such that  $M \subsetneq B \subseteq R$ .

Let  $b \in B, b \notin M$ .

$\therefore R/M$  is a field

$$\therefore b + M \in R/M, b + M \neq M$$

$\therefore R/M$  is a field.

$\therefore 1 + M \in R/M$  and every nonzero element of  $R/M$  has a multiplicative inverse.

Hence,  $\exists \bar{c} = c + M \in R/M$  s.t.  $(b + M)(c + M) = 1 + M$

$$\Rightarrow bc + M = 1 + M$$

Since,  $R/M$  is a field, then the cancellation laws



(ii) proving that:

$R/M$  is a field  $\Rightarrow M$  is a maximal ideal of  $R$ .

Let  $R/M$  be a field.

Suppose that  $B$  is an ideal of  $R$  such that  $M \subset B \subseteq R$ .  $\therefore$

Let  $b \in B$ ,  $b \notin M$ .

$\therefore b+M \in R/M$ ,  $b+M \neq M$  i.e.  $\bar{b} \neq \bar{0}$

Because (1)  $R/M = \{r+M \mid r \in R\}$

(2)  $b \in B$ ,  $B \subseteq R \Rightarrow b \in R \Rightarrow$  put  $r = b$

$\therefore R/M$  is a field.

$\therefore 1+M \in R/M$  and every nonzero element of  $R/M$  is a unit.

$\therefore \exists \bar{a} = a+M \in R/M \Rightarrow ab+M = 1+M$

( $\bar{a} \neq \bar{0}$ ) i.e.  $\bar{a} \cdot \bar{b} = \bar{1} \Rightarrow \boxed{a \cdot b = 1} \rightarrow \textcircled{*}$

$\therefore b \in B$ ,  $B \subseteq R$ .

$\therefore r \cdot b \in B \forall r \in R$ .

Put  $r = a$ .

$\therefore ab \in B$

$\therefore ab = 1$  (from  $\textcircled{*}$ )

$\therefore 1 \in B$ .

$\therefore 1 \in B \Rightarrow 1 \cdot r \in B \forall r \in R \Rightarrow R \subseteq B$  but  $B \subseteq R$   
 $\Rightarrow R = B$

$\therefore B = R$  (theorem)

$\therefore M$  is a maximal ideal of  $R$ .



hold.

$$\Rightarrow (bc+M) + (-1+M) = (1+M) + (-1+M)$$

$$\Rightarrow (bc-1) + M = (1-1) + M$$

$$\Rightarrow (bc-1) + M = 0 + M.$$

$$\Rightarrow (bc-1) + M = M$$

$$\therefore bc-1 \in M$$

$$\therefore b \in B, bc=1$$

$$\therefore bc \in B \text{ (as } B \triangleleft R \Rightarrow B \leq R)$$

$$\therefore M \subset B, bc-1 \in M.$$

$$\therefore bc-1 \in B.$$

$$\therefore B \triangleleft R$$

$$\therefore a-b \in B \quad \forall a, b \in B$$

$$\Rightarrow bc - (bc-1) \in B$$

$$\Rightarrow 1 \in B.$$

$$\therefore B \triangleleft R, 1 \in B.$$

$$\therefore B = R \text{ (Theorem)}$$

$\Rightarrow M$  is a maximal ideal.

(II)  $I \triangleleft R$ ,  $I$  is prime  $\Rightarrow R/I$  is an integral <sup>domain</sup> ~~today~~.  
Let  $R$  be a commutative ring with unity and  $I$  be an ideal of  $R$ .

(i) proving that:

$R/I$  an integral domain  $\Rightarrow I$  is a prime ideal of  $R$ .

Let  $R/I$  be an integral domain.

Let  $a, b \in R \nexists ab \in I$

Now, we need to prove that  $a \in I$  or  $b \in I$ .

$$\therefore ab \in I$$

$$\therefore ab + I = (a + I) \cdot (b + I) = I$$

$\therefore R/I$  is an integral domain.



$\therefore R/I$  has no zero divisors.

$\Rightarrow a+I = I$  or  $b+I = I$ .

$\Rightarrow a \in I$  or  $b \in I$ .

$\therefore I$  is a prime ideal.

(ii) Proving that:

$I$  is a prime ideal of  $R \Rightarrow R/I$  is an integral domain  
Let  $I$  be a prime ideal of  $R$ .

$\therefore R$  is a commutative ring with unity.

$\therefore R/I$  is a commutative ring with unity.

To prove that  $R/I$  is an integral domain, all we need to prove is that  $R/I$  has no zero divisors.

Let  $a+I, b+I \in R/I \exists (a+I)(b+I) = I$

$\Rightarrow ab+I = I \Rightarrow ab \in I$ .

$\therefore I$  is a prime ideal of  $R$ .

$\therefore a \in I$  or  $b \in I$

$\Rightarrow a+I = I$  or  $b+I = I$

$\therefore R/I$  has no zero divisors.

$\therefore R/I$  is an integral domain.

(III)  $M \triangleleft R$ ,  $M$  is maximal  $\Rightarrow M$  is prime.

Let  $M$  be a maximal ideal of  $R$ .

$\Rightarrow R/M$  is a field. (from I.)

Since, every field is an integral domain

$\Rightarrow R/M$  is an integral domain.

$\Rightarrow M$  is a prime ideal. (from II)

~~Corollary~~ Corollary:

A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

proof:



■ proof:

(i) proving that:

$F$  is a field  $\Rightarrow F$  has no proper nontrivial ideal.  
Let  $F$  be a field and  $N$  be an ideal of  $F$  ( $N \triangleleft F$ )  
such that  $N \neq \{0\}$ .

Since every nonzero element of a field is a unit.

Hence,  $\exists u \in N, u' \in F \ni uu' \in N \Rightarrow 1 \in N$

$\Rightarrow r \cdot 1 \in N \forall r \in F \Rightarrow r \in N \forall r \in F$

$\therefore N \supseteq F \rightarrow (1)$

$\therefore N \triangleleft F \quad \therefore N \leq F \Rightarrow N \subseteq F \rightarrow (2)$

from (1) and (2)  $\Rightarrow N = F$ .

$\therefore F$  has no proper nontrivial ideals.

(ii) proving that:

$R$  is a commutative ring with unity and has no proper nontrivial ideals  $\Rightarrow R$  is a field.

Let  $R$  be a commutative ring with unity and has no proper nontrivial ideals.

To prove that  $R$  is a field, all we need to do is to prove that every nonzero element of  $R$  is a unit.

Let  $a \neq 0 \in R$ .

Define  $Ra = \{ra \mid r \in R\} \triangleleft R$

$\therefore R$  has no proper nontrivial ideals.

$\therefore Ra = R$

$\therefore 1 \in R \quad \therefore 1 \in Ra$

$\Rightarrow \exists b \neq 0 \in R \ni ab = 1$ .

$\Rightarrow a$  is a unit.

$\therefore R$  is a field.



## 2) prime Fields :

### I. Theorem:

If  $R$  is a ring with unity (1), then the mapping

$\Phi: \mathbb{Z} \rightarrow R$  given by

$\Phi(n) = n \cdot 1$  for  $n \in \mathbb{Z}$  is a homomorphism.

■ proof:

$$(i) \Phi(n+m) = (n+m) \cdot 1 = (n \cdot 1) + (m \cdot 1) = \Phi(n) + \Phi(m)$$

$$(ii) \Phi(nm) = (nm) \cdot 1 = (n \cdot 1)(m \cdot 1) = \Phi(n) \Phi(m).$$

### II. Corollary:

If  $R$  is a ring with unity and  $\text{ch}(R) = n > 1$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}_n$ .

If  $R$  has  $\text{ch}(R) = 0$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}$ .

■ proof:

The mapping  $\Phi: \mathbb{Z} \rightarrow R$   $\exists$   $\Phi(n) = n \cdot 1$  is a homomorphism.

Hence, the kernel  $[\text{Ker}(\Phi)]$  must be an ideal of  $\mathbb{Z}$ .

But all ideals of  $\mathbb{Z}$  are of the form  $S\mathbb{Z}$  for some  $S \in \mathbb{Z}$ .

also we know that:

If  $R$  has  $\text{ch}(R) = n > 0$ , then  $\text{Ker}(\Phi) = n\mathbb{Z}$  (theorem)

$\Rightarrow \Phi(\mathbb{Z})$  subring of  $R$  (i.e.  $\Phi(\mathbb{Z}) \leq R$ ) is isomorphic to  $\mathbb{Z}/\text{Ker}(\Phi)$ .

i.e.  $\Phi(\mathbb{Z}) \cong \mathbb{Z}/\text{Ker}(\Phi)$ .

$\Rightarrow \Phi(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ .

But  $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n \Rightarrow \Phi(\mathbb{Z}) \cong \mathbb{Z}_n$

If  $\text{ch}(R) = 0 \Rightarrow \text{Ker}(\Phi) = \{0\}$



$$\Rightarrow \phi(\mathbb{Z}) \cong \mathbb{Z}/\{0\} \cong \mathbb{Z} \neq$$

### (3) Rings of polynomials:

#### I. Polynomial:

Let  $R$  be a ring. A polynomial  $f(x)$  with coefficients in  $R$  can be given as:

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots$$

where,  $a_i \in R$ ,  $a_i \neq 0$  for a finite number of  $i$ .

The degree of the polynomial  $f(x) = n$ , denoted by  $\deg[f(x)] = n$ , when;

$$f(x) = \sum_{i=0}^{\infty} a_i x^i, a_n \neq 0 \text{ and } a_i = 0 \forall i > n$$

$$\therefore \deg[f(x)] = n \iff f(x) = \sum_{i=0}^n a_i x^i, a_n \neq 0$$

#### II. Ring of polynomial:

Let  $R$  be a ring, and  $R[x]$  denote the set of all polynomials with coefficients in  $R$ , where

$$R[x] = \left\{ \sum_{i=0}^{\infty} a_i x^i \mid a_i \in R \right\}$$

Then  $(R[x], +, \cdot)$  constitutes a ring called "the ring of polynomials" where  $(+)$  and  $(\cdot)$  are the addition and multiplication of polynomials.

#### III. properties of addition and multiplication of polynomials:

Let  $f(x), g(x) \in R[x]$ , where

$$f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i, a_i, b_i \in R$$

$$(1) f(x) + g(x) = \sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$



$$= \sum_{i=0}^{\infty} c_i x^i \quad \& \quad c_i = a_i + b_i \quad \forall i$$

$$\text{Let } \deg[f(x)] = n, \deg[g(x)] = m.$$

$$\Rightarrow \deg[f(x) + g(x)] \leq \max[\deg[f(x)], \deg[g(x)]] = \max[m, n].$$

$$(2) f(x)g(x) = \sum_{i=0}^{\infty} a_i x^i \cdot \sum_{i=0}^{\infty} b_i x^i = \sum_{n=0}^{\infty} \left( \sum_{i=0}^n a_i b_{n-i} \right) x^n \\ = \sum_{n=0}^{\infty} d_n x^n \quad \& \quad d_n = \sum_{i=0}^n a_i b_{n-i}$$

$$\Rightarrow \deg[f(x)g(x)] \leq \{\deg[f(x)] + \deg[g(x)] = n + m\}.$$

#### IV. Theorem:

(1)  $R$  is a ring  $\Rightarrow R[x]$  is a ring.

(2)  $R$  is commutative ring  $\Rightarrow R[x]$  is a commutative ring.

(3)  $R$  is a ring with unity  $\Rightarrow R[x]$  is a ring with unity.

(4)  $R$  is an integral domain  $\Rightarrow R[x]$  is an integral domain.

(5)  $R$  is a field  $\Rightarrow R[x]$  is an integral domain.

$\hookrightarrow R$  is a field  $\not\Rightarrow R[x]$  is a field.



\* Day: Tuesday

\* Subject: Abstract algebra (3)

\* Date: 3/3/2015

\* Lecture: 3

### (1) Theorem (1):

I. If  $R$  is an integral domain (I.D.), then  $R[x]$  is an integral domain.

i.e.  $R = \text{I.D.} \Rightarrow R[x] = \text{I.D.}$

■ proof:

→ Remark: An integral domain is a commutative ring with unity (1) and has no zero divisors.

Let  $R$  be an integral domain.

$\therefore R[x]$  is a commutative ring with unity (1)

Hence, all we need to do is to prove that  $R[x]$  has no zero divisors.

Let  $f(x), g(x) \in R[x]$  such that;

$$f(x) = a_0 + a_1x + \dots + a_nx^n, a_n \neq 0$$

$$g(x) = b_0 + b_1x + \dots + b_mx^m, b_m \neq 0$$

$\Rightarrow f(x)g(x) \neq 0$  because  $a_n, b_m \neq 0$  as  $R$  has no zero divisors.

$\therefore R[x]$  has no zero divisors.

$\therefore R[x]$  is an integral domain.

II. If  $R$  is a field, then  $R[x]$  is an integral domain but not a field.

■ proof:

Let  $R$  be a field.

$\therefore$  Every field is an integral domain.



$\therefore R$  is an integral domain.

Hence, from theorem (I.)  $\Rightarrow R[x]$  is an integral domain.

But  $R[x]$  isn't a field because;

$$\nexists g(x) \in R[x] \ni x \cdot g(x) = 1$$

$\therefore f(x) = x$  has no multiplicative inverse (i.e.  $x$  isn't a unit)

$\therefore R[x]$  isn't a field.

## (2) Equality of two polynomials:

$$\text{Let } f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i.$$

$$\text{If } g(x) = f(x), \text{ then } \sum_{i=0}^{\infty} a_i x^i = \sum_{i=0}^{\infty} b_i x^i$$

$$\Rightarrow \sum_{i=0}^{\infty} a_i x^i - \sum_{i=0}^{\infty} b_i x^i = 0 \Rightarrow \sum_{i=0}^{\infty} (a_i - b_i) x^i = 0$$

$$\Rightarrow a_i - b_i = 0 \quad \forall i \Rightarrow a_i = b_i \quad \forall i$$

$$\Rightarrow \deg[f(x)] = \deg[g(x)]$$

## (3) Units of an integral domain of polynomials:

### **I. Theorem:**

If  $R$  is an integral domain, then units of  $R[x]$  are the same as the units of  $R$ .

■ proof:

Let  $R$  be an integral domain.



suppose that  $\exists f(x), g(x) \in R[x] \ni f(x)g(x) = 1$

\* Remark:

we know that if  $R[x]$  is a ring of polynomials and  $f(x), g(x) \in R[x]$ , then

$$\deg[f(x) \cdot g(x)] \leq \deg[f(x)] + \deg[g(x)]$$

But if  $R[x]$  is an integral domain (i.e. has no zero divisors), then:

$$(i) \deg[f(x) \cdot g(x)] = \deg[f(x)] + \deg[g(x)]$$

$$(ii) \deg[f(x) + g(x)] \leq \max\{\deg[f(x)], \deg[g(x)]\}$$

\* Going back to the proof

$$\therefore f(x) \cdot g(x) = 1$$

$$\therefore \deg[f(x) \cdot g(x)] = \deg[1] = 0$$

$$\text{But } \deg[f(x)g(x)] = \deg[f(x)] + \deg[g(x)]$$

$$\therefore \deg[f(x)] + \deg[g(x)] = 0$$

$$\Rightarrow \deg[f(x)] = \deg[g(x)] = 0$$

$$\Rightarrow f(x) = u, g(x) = v, u, v \in R$$

$$\therefore uv = 1, u, v \in R$$

$$\therefore u, v \text{ are units of } R$$

II. Remark:

If  $R$  isn't an integral domain, then units of  $R[x]$  not necessarily are the same as those of  $R$ .  
for example:

In  $\mathbb{K}_4[x]$ , we have

$$(2x+1)(2x+1) = 4x^2 + 4x + 1 = 1$$

$\Rightarrow (2x+1)$  is a unit of  $\mathbb{K}_4[x]$  but not a unit of  $\mathbb{K}_4$ .



#### (4) Zero of a polynomial:

Let  $R[x]$  be a ring of polynomials.

Suppose that  $f(x) \in R[x]$  such that

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$$

Let  $\alpha \in R$ .

If  $f(\alpha) = 0$ , then  $\alpha$  is called "Zero of the polynomial  $f(x)$ ".

$$\text{where } f(\alpha) = \sum_{i=0}^n a_i \alpha^i = a_0 + a_1 \alpha + a_2 \alpha^2 + \dots + a_n \alpha^n$$

#### (5) Theorem (2): (The evaluation homomorphism):

I. Theorem:

Let  $F$  be a subfield of a field  $E$  (i.e.  $F \subseteq E$ ). Let  $\alpha$  be any element of  $E$  (i.e.  $\alpha \in E$ ).

The map;  $\Phi_\alpha: F[x] \longrightarrow E$  where;

$$\Phi_\alpha[f(x)] = f(\alpha) \text{ is a homomorphism.}$$

■ proof:

we need to prove that:

$$\Phi_\alpha[f(x) + g(x)] = \Phi_\alpha[f(x)] + \Phi_\alpha[g(x)]$$

$$\Phi_\alpha[f(x)g(x)] = \Phi_\alpha[f(x)] \cdot \Phi_\alpha[g(x)]$$

$$\text{Let } f(x), g(x) \in F[x] \text{ s.t. } f(x) = \sum_{i=0}^{\infty} a_i x^i, g(x) = \sum_{i=0}^{\infty} b_i x^i$$

$$(i) \Phi_\alpha[f(x) + g(x)] = \Phi_\alpha\left[\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i\right] =$$



$$\begin{aligned}
 &= \Phi_{\alpha} \left[ \sum_{i=0}^{\infty} (a_i + b_i) x^i \right] = \sum_{i=0}^{\infty} (a_i + b_i) \alpha^i = \\
 &\sum_{i=0}^{\infty} a_i \alpha^i + \sum_{i=0}^{\infty} b_i \alpha^i = f(\alpha) + g(\alpha) = \\
 &= \Phi_{\alpha}[f(x)] + \Phi_{\alpha}[g(x)].
 \end{aligned}$$

$$\begin{aligned}
 \text{(ii)} \quad \Phi_{\alpha}[f(x) \cdot g(x)] &= \Phi_{\alpha} \left[ \sum_{i=0}^{\infty} a_i x^i \cdot \sum_{i=0}^{\infty} b_i x^i \right] = \\
 &\Phi_{\alpha} \left[ \sum_{n=0}^{\infty} \left( \sum_{i=0}^n a_i b_{n-i} \right) x^n \right]
 \end{aligned}$$

$$\text{Let } d_n = \sum_{i=0}^n a_i b_{n-i}$$

$$\begin{aligned}
 \Rightarrow \Phi_{\alpha}[f(x) \cdot g(x)] &= \Phi_{\alpha} \left[ \sum_{n=0}^{\infty} d_n x^n \right] = \sum_{n=0}^{\infty} d_n \alpha^n \\
 &= \left( \sum_{i=0}^{\infty} a_i \alpha^i \right) \left( \sum_{i=0}^{\infty} b_i \alpha^i \right) = f(\alpha) g(\alpha) = \\
 &= \Phi_{\alpha}[f(x)] \cdot \Phi_{\alpha}[g(x)].
 \end{aligned}$$

From (i) and (ii)  $\Rightarrow \Phi_{\alpha}$  is a homomorphism

► Examples:

Let  $F = \mathbb{Q}$ ,  $E = \mathbb{R} \ni \Phi : \mathbb{Q}[x] \rightarrow \mathbb{R}$

$$\text{(i)} \quad \Phi_0[f(x)] = \Phi_0[a_0 + a_1 x + \dots + a_n x^n] = f(0) = a_0.$$

$$\text{(ii)} \quad \Phi_2[f(x)] = \Phi_2[a_0 + a_1 x + \dots + a_n x^n] = a_0 + 2a_1 + \dots + 2^n a_n$$

$$\text{(iii)} \quad \Phi_0[g(x)] = \Phi_0[x^2 + 2x + 1] = 0^2 + 2(0) + 1 = 1.$$

$$\text{(iv)} \quad \Phi_2[h(x)] = \Phi_2[x + 1] = 2 + 1 = 3.$$

$$\text{(v)} \quad \Phi_{\sqrt{2}}[k(x)] = \Phi_{\sqrt{2}}[x^2 + x] = (\sqrt{2})^2 + \sqrt{2} = 2 + \sqrt{2}$$

II. Remark:

$$\text{Let } \Phi_{\alpha} : F[x] \rightarrow E \ni \Phi_{\alpha}[f(x)] = f(\alpha).$$



Then, the kernel of  $\Phi_a$  is given as:

$$\ker[\Phi_a] = \{f(x) \in F[x] \ni \Phi_a[f(x)] = 0\}$$

► Examples:

(1)  $\Phi_2: \mathbb{Q}[x] \longrightarrow \mathbb{R}$

Let  $f(x) \in \mathbb{Q}[x] \ni f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \dots + a_n x^n$   
 $\Phi_2[f(x)] = a_0 + 2a_1 + \dots + 2^n a_n$

$$\ker[\Phi_2] = \{f(x) \in \mathbb{Q}[x] \ni \Phi_2[f(x)] = f(2) = 0\}$$

we find that the polynomial  $g(x) = x^2 + x - 6 \in \ker(\Phi_2)$

where  $\Phi_2[g(x)] = g(2) = (2)^2 + 2 - 6 = 6 - 6 = 0$ .

(2) Let  $\Phi_2: \mathbb{K}_7[x] \longrightarrow \mathbb{K}_7$

Compute the indicated evaluation homomorphism

(i)  $\Phi_2(x^2 + 3) = (2)^2 + 3 = 4 + 3 = 7 = 0$

$$\Rightarrow x^2 + 3 \in \ker[\Phi_2]$$

(ii)  $\Phi_2(2x^3 - x^2 + 3x + 2) = 2(2)^3 - (2)^2 + 3(2) + 2 = 2$

(3) Let  $\Phi_5: \mathbb{Q}[x] \longrightarrow \mathbb{R}$

Find six elements in the kernel of  $\Phi_5$ .

$$\ker[\Phi_5] = \{f(x) \in \mathbb{Q}[x] \ni \Phi_5[f(x)] = f(5) = 0\}$$

→ Hence work.

«(Solution)»

we need to find  $f(x) \in \mathbb{Q}[x] \ni f(5) = 0$

Let  $f(x) = kx - t$

$$\Rightarrow f(5) = 5k - t$$

$$\text{Put } f(5) = 0 \Rightarrow 5k - t = 0 \Rightarrow t = 5k$$

$\therefore$  all polynomials of the form;

$f_k(x) = kx - t \ni k, t \in \mathbb{K}^+, t = 5k$  belong to the kernel of  $\Phi_5$



for example:

$$(i) f_1(x) = 1(x) - 5(1) = x - 5$$

$$\Rightarrow f_1(5) = 5 - 5 = 0 \Rightarrow f_1(x) \in \ker(\Phi_5)$$

$$(ii) f_2(x) = 2(x) - 5(2) = 2x - 10$$

$$\Rightarrow f_2(5) = 2(5) - 10 = 10 - 10 = 0 \Rightarrow f_2(x) \in \ker(\Phi_5)$$

and so on.

also, let  $f(x) = \frac{\mu}{k^i} x^i - \mu$ ,  $k, \mu$  are constants

$$\Rightarrow f(5) = \frac{\mu}{k^i} (5)^i - \mu$$

$$\text{put } f(5) = 0 \Rightarrow \frac{\mu}{k^i} (5)^i - \mu = 0$$

$$\Rightarrow \frac{\mu}{k^i} (5)^i = \mu \Rightarrow \frac{1}{k^i} (5)^i = 1 \Rightarrow (5)^i = k^i$$

$$\therefore k = 5.$$

Hence, all polynomials of the form:

$$f_n(x) = \frac{\mu}{5^n} x^n - \mu \quad \exists n \in \mathbb{N}^*, \mu \in \mathbb{R}$$

belong to the kernel of  $\Phi_5$ .

for example:

$$f_1(x) = \frac{\mu}{5} x - \mu = \frac{1}{5} \mu x - \mu = \mu \left( \frac{1}{5} x - 1 \right)$$

$$\Rightarrow \Phi_5[f_1(x)] = f_1(5) = \mu \left( \frac{1}{5}(5) - 1 \right) = \mu(1 - 1) = \mu(0) = 0.$$

$$\therefore f_1(x) \in \ker(\Phi_5).$$

and so on.

II. Theorem (3):

The equation  $x^2 = 2$  has no solutions in the set of



rational numbers  $\mathbb{Q}$ . Thus  $\sqrt{2}$  isn't a rational number.

## 6) Factorization of polynomials over a field:

Let  $E$  and  $F$  be fields such that  $F \subseteq E$ .

Suppose that  $f(x) \in F[x]$  factors in  $F[x]$ , so that  $f(x) = g(x)h(x)$  where  $g(x), h(x) \in F[x]$ .

Let  $\alpha \in E$ . Now for the evaluation homomorphism  $\Phi_\alpha$ , where:

$$\Phi_\alpha[f(x)] = f(\alpha) = \Phi_\alpha[g(x)h(x)] = \Phi_\alpha[g(x)] \cdot \Phi_\alpha[h(x)] = g(\alpha) \cdot h(\alpha).$$

Hence,  $f(\alpha) = 0$  if and only if  $g(\alpha) = 0$  or  $h(\alpha) = 0$ . Since we are concerned with finding zeroes of polynomials, now our problem is reduced to finding a zero of a factor of  $f(x)$ .

### I. Theorem (1): (Division algorithm for $F[x]$ )

Let  $F$  be a field.

Suppose that  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$$

are two elements of  $F[x]$  with both  $a_n$  and  $b_m$  are non zero elements of  $F$  and  $m > 0$ .

Then, there are unique polynomials  $q(x)$  and  $r(x)$  in  $F[x]$  such that  $f(x) = g(x)q(x) + r(x)$ .

with the degree of  $r(x)$  less than the degree of  $g(x) = m$ .

Briefly;

Let  $f(x), g(x) \in F[x]$ , then  $\exists$  unique  $q(x), r(x) \in F[x]$

$$\text{such that } f(x) = g(x)q(x) + r(x) \text{ and } \deg[r(x)] < \deg[g(x)].$$



■ proof:

$$\text{Let } f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0.$$

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_0.$$

Consider the set  $S = \{ f(x) - g(x)s(x) \mid s(x) \in F[x] \}$ .

Let  $r(x) \in S$  such that  $r(x)$  of minimal degree.

$$\therefore r(x) \in S \quad \therefore \exists q(x) \in F[x] \ni r(x) = f(x) - g(x)q(x)$$

$$\Rightarrow f(x) = g(x)q(x) + r(x).$$

we must show that the degree of  $r(x)$  is less than the degree of  $g(x) = m$ .

Suppose that;

$$r(x) = c_t x^t + c_{t-1} x^{t-1} + \dots + c_0 \quad \exists c_i \in F, r(x) \in F[x], \\ c_t \neq 0 \text{ if } t \neq 0.$$

if  $t \geq m$ , then:

$$r(x) - \frac{c_t}{b_m} x^{t-m} g(x) = f(x) - g(x)q(x) - \frac{c_t}{b_m} x^{t-m} g(x)$$

$$\Rightarrow f(x) - g(x)q(x) - \frac{c_t}{b_m} x^{t-m} g(x) = r(x) - (c_t x^t + \text{terms of lower degree}).$$

$$\Rightarrow \deg \left\{ f(x) - g(x)q(x) - \frac{c_t}{b_m} x^{t-m} g(x) \right\} < \deg \{ r(x) - (c_t x^t + \dots) \} = t$$

But the left hand side of the previous equation can be written as;  $f(x) - g(x) \left[ q(x) + \frac{c_t}{b_m} x^{t-m} \right] \in S$  with degree  $< t$ .

which is contradiction to our choice to  $r(x)$  as of minimal degree.

$$\therefore m > t.$$

Now, we prove the uniqueness;

$$\text{Let } f(x) = g(x)q_1(x) + r_1(x)$$

$$\text{and } f(x) = g(x)q_2(x) + r_2(x)$$



$$\Rightarrow g(x)q_1(x) + r_1(x) = g(x)q_2(x) + r_2(x)$$

$$\Rightarrow g(x)[q_1(x) - q_2(x)] = r_2(x) - r_1(x)$$

$$\Rightarrow \deg[g(x)(q_1(x) - q_2(x))] = \deg[r_2(x) - r_1(x)]$$

Since  $g(x), q_1(x), q_2(x), r_1(x), r_2(x) \in F[x]$  which is an integral domain.

$$\therefore \deg[g(x)] + \deg[q_1(x) - q_2(x)] = \deg[r_2(x) - r_1(x)]$$

$$\text{but } \deg[r_2(x) - r_1(x)] < \deg[g(x)]$$

$$\therefore \deg[r_2(x) - r_1(x)] = \deg[q_1(x) - q_2(x)] = 0$$

$$\therefore r_1(x) = r_2(x) \text{ and } q_1(x) = q_2(x). \quad \#$$

II. Corollary:

an element  $a \in F$  is a zero of  $f(x) \in F[x]$  if and only if  $(x-a)$  is a factor of  $f(x)$  in  $F[x]$ .

Proof:

(i) proving that:

$a \in F$  is a zero of  $f(x) \Rightarrow (x-a)$  is a factor of  $f(x)$ .

Let  $a \in F$  be a zero of  $f(x) \in F[x]$ .

$$\Rightarrow f(a) = 0$$

By division algorithm

$$\Rightarrow f(x) = (x-a)q(x) + r(x).$$

$$\therefore \deg[r(x)] < \deg[x-a] = 1$$

$$\therefore \deg[r(x)] < 1 \Rightarrow \deg[r(x)] = 0 \Rightarrow r(x) = c.$$



$$\Rightarrow f(x) = (x-a)g(x) + c$$

$\therefore a$  is a zero of  $f(x)$ .

$$\therefore f(a) = 0 \Rightarrow 0 = (a-a)g(a) + c$$

$$\Rightarrow c = 0.$$

$$\therefore f(x) = (x-a)g(x).$$

$\therefore (x-a)$  is a factor for  $f(x)$ .

(ii) proving that:

$(x-a)$  is a factor of  $f(x) \Rightarrow a$  is a zero of  $f(x)$ .

Let  $(x-a)$  be a factor of  $f(x)$ .

$$\therefore f(x) = (x-a)g(x)$$

By applying the evaluation homomorphism  $\Phi_a[f(x)]$  we get:

$$\Phi_a[f(x)] = f(a) = (a-a)g(a) = 0g(a) = 0$$

$\therefore a$  is a zero of  $f(x)$ . #

➤ Example:

Let  $f(x), g(x) \in \mathbb{K}_5[x]$  such that

$$f(x) = x^4 - 3x^3 + 2x^2 + 4x - 1$$

$$g(x) = x^2 - 2x + 3$$

find  $q(x), r(x)$  s.t.  $f(x) = g(x)q(x) + r(x)$ .

→ Homework.



⊗ Day: Tuesday

⊗ Date: 10/3/2015

⊗ Subject: Abstract algebra (3)

⊗ Lecture: 4

## (1) Irreducible polynomials

### I. Definition: (Irreducible polynomials)

Let  $F$  be a field.

A nonconstant polynomial  $f(x) \in F[x]$  is irreducible over  $F$  (or is an irreducible polynomial in  $F[x]$ ) if  $f(x)$  can't be expressed as a product  $g(x)h(x)$  of two polynomials  $g(x)$  and  $h(x)$  in  $F[x]$  both of lower degree than the degree of  $f(x)$ .

### II. Remark:

Let  $F$  be a subfield of  $E$  (i.e.  $F \leq E$ ).

A polynomial  $f(x)$  may be irreducible over  $F$ , but may not be irreducible over  $E$ .

### ➤ Example:

(1) The polynomial  $[f(x) = x^2 - 2]$  has no zeroes in  $\mathbb{Q}$ , this implies that  $f(x)$  is irreducible over  $\mathbb{Q}$ . However  $f(x)$  is reducible over  $\mathbb{R}$  because  $f(x)$  factors in  $\mathbb{R}[x]$  into  $(x - \sqrt{2})(x + \sqrt{2})$ .



2) The polynomial  $g(x) = x^2 + 2$  has no zeroes in  $\mathbb{R}$  and this implies that  $g(x)$  is irreducible over  $\mathbb{R}$ . However  $g(x)$  is reducible over  $\mathbb{C}$  because it factors in  $\mathbb{C}[x]$  into  $(x + \sqrt{2}i)(x - \sqrt{2}i)$ .

3) The polynomial  $g(x) = x^3 + 3x + 2 \in \mathbb{K}_5[x]$  is irreducible over  $\mathbb{K}_5$  because it has no zeroes in  $\mathbb{K}_5$ ; where:

$$\mathbb{K}_5 = \{0, 1, 2, 3, 4\}$$

$$g(0) = (0)^3 + 3(0) + 2 = 2 \neq 0$$

$$g(1) = (1)^3 + 3(1) + 2 = 6 = 1 \neq 0$$

$$g(2) = (2)^3 + 3(2) + 2 = 16 = 1 \neq 0$$

$$g(3) = (3)^3 + 3(3) + 2 = 38 = 3 \neq 0$$

$$g(4) = (4)^3 + 3(4) + 2 = 78 = 3 \neq 0$$

~~$g(x) = x^3 + 3x + 2$~~

### III. Theorem (1):

Let  $F$  be a field and let  $f(x) \in F[x]$  where  $f(x)$  is of degree 2 or 3.

Then  $f(x)$  is reducible over  $F$  if and only if it has a zero in  $F$ .

□ proof:

Let  $F$  be a field and  $f(x) \in F[x]$ , where  $f(x)$  of degree 2 or 3.

(i) proving that:

$f(x)$  is reducible over  $F \Rightarrow f(x)$  has a zero in  $F$ .



Let  $f(x)$  be reducible over  $F$ .

Then,  $\exists g(x), h(x) \in F[x] \ni f(x) = g(x)h(x)$   
where the degree of both  $g(x)$  and  $h(x)$  is less than the degree of  $f(x)$  which is 2 or 3, hence either  $g(x)$  or  $h(x)$  is of degree 1, say  $g(x)$  is of degree 1, hence  $g(x)$  is of the form  $g(x) = x - a$  where  $a \in F$ .

$$\Rightarrow f(x) = (x - a)h(x)$$

Applying the evaluation homomorphism to  $f(x)$  at  $x = a$

$$\Rightarrow \phi_a[f(x)] = f(a) = (a - a)h(a) = 0(h(a)) = 0.$$

$\Rightarrow a$  is a zero of  $f(x)$ .

$\therefore f(x)$  has a zero in  $F$ .

(ii) proving that:

$f(x)$  has a zero in  $F \Rightarrow f(x)$  is reducible over  $F$ .

Let  $f(x)$  has a zero in  $F$ , say  $a$ .

$$\Rightarrow \phi_a[f(x)] = f(a) = 0.$$

hence,  $f(x)$  can be reformed as:

$$f(x) = (x - a)q(x) + r(x)$$

and the degree of  $r(x)$  is less than the degree of  $(x - a)$  which is equal to 1, thus the degree of  $r(x)$  is zero.

$$\therefore r(x) = c$$

$$\Rightarrow f(x) = (x - a)q(x) + c$$

$\therefore a$  is a zero of  $f(x)$ ;

$$\therefore f(a) = 0$$

$$\Rightarrow (a - a)q(a) + c = 0 \Rightarrow c = 0.$$

$$\Rightarrow f(x) = (x - a)q(x)$$



$\therefore (x-a)$  is a factor of  $f(x)$ .

So,  $f(x)$  is reducible over  $F$ .

➤ Example :

The polynomial  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$  is irreducible over  $\mathbb{Q}$  because it has no zeroes in  $\mathbb{Q}$ .

#### IV. Theorem (2) :

If  $f(x) \in \mathbb{K}[x]$ , then  $f(x)$  factors into a product of two polynomials of lower degrees  $r$  and  $s$  in  $\mathbb{Q}[x]$  if and only if it has such a factorization with polynomials of the same degrees  $r$  and  $s$  in  $\mathbb{K}[x]$ .

#### V. Corollary :

If  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$  is in  $\mathbb{K}[x]$  with  $a_0 \neq 0$ , and if  $f(x)$  has a zero in  $\mathbb{Q}$ , then it has a zero  $m$  in  $\mathbb{K}$  and  $m$  must divide  $a_0$ .

▣ proof :

Let  $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{K}[x]$ ,  $a_0 \neq 0$ .

Suppose that  $f(x)$  has a zero  $(\alpha)$  in  $\mathbb{Q}$ .

$\therefore f(x)$  has a linear factor  $(x-a)$  in  $\mathbb{Q}[x]$  (Corollary states that "An element  $a \in F$  is a zero of  $f(x) \in F[x]$  if and only if



$(x-a)$  is a factor of  $f(x)$  in  $F[x]$ ."

But by the previous theorem (IV. theorem (2))  $f(x)$  has a factorization with a linear factor in  $K[x]$ , so for some  $m \in K$  we must have

$$f(x) = (x-m)(x^{n-1} + \dots + a_0/m)$$

$$\therefore a_0/m \in K$$

$\therefore m$  must divide  $a_0$  #.

### ➤ Examples :

(1) The polynomial  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$  has a zero in  $\mathbb{Q}$  if and only if it has a zero ( $m$ ) in  $K$  satisfying that  $m \mid -2$ .

$$\Rightarrow m = \pm 1 \quad \text{or} \quad m = \pm 2.$$

$$f(\pm 1) = 1 - 2 = -1 \neq 0$$

$$f(\pm 2) = 4 - 2 = 2 \neq 0$$

$\therefore \nexists m \in K \ni m \mid a_0$  and  $f(m) = 0$ .

$\therefore f(x)$  is irreducible over  $\mathbb{Q}$ .

(2) Show that  $f(x) = x^4 - 2x^2 + 8x + 1 \in \mathbb{Q}[x]$  is irreducible over  $\mathbb{Q}$ .

(i) If  $f(x)$  has a linear factor in  $\mathbb{Q}[x]$ , then it has a zero in  $K$ . Say  $m$ , satisfying that  $m \mid 1$ .

$$\Rightarrow m = \pm 1$$

$$f(1) = (1)^4 - 2(1)^2 + 8(1) + 1 = 8 \neq 0$$

$$f(-1) = (-1)^4 - 2(-1)^2 + 8(-1) + 1 = -8 \neq 0$$

$\therefore f(x)$  has no zeroes in  $\mathbb{Q}$ .



52) such a factorization is impossible.

(ii) If  $f(x)$  factors into two quadratic factors in  $\mathbb{Q}[x]$ , then it has a factorization of the form:

$$f(x) = (x^2 + ax + b)(x^2 + cx + d) \text{ where } a, b, c, d \in \mathbb{K}.$$

$$\Rightarrow x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd = x^4 - 2x^2 + 8x + 1$$

By comparing the coefficients of both sides;

$$a+c=0, \quad ad+bc=8$$

$$b+d+ac=-2, \quad bd=1$$

$$\therefore b, d \in \mathbb{K}, \quad bd=1$$

$$\therefore b=d=1 \text{ or } b=d=-1.$$

$$\text{at } b=d=1$$

$$\therefore ad+bc=8$$

$$\therefore a(1)+c(1)=8 \Rightarrow a+c=8 \text{ but we have}$$

$$a+c=0 \text{ which is contradiction.}$$

$$\text{at } b=d=-1$$

$$\Rightarrow -a-c=8 \Rightarrow a+c=-8 \text{ but } a+c=0$$

$$\text{which is contradiction again.}$$

$$\therefore f(x) \text{ is irreducible over } \mathbb{Q}.$$

## VI. Theorem (3): (Eisenstein)

Let  $p \in \mathbb{K}$  be a prime.

Suppose that  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  is in  $\mathbb{K}[x]$

and:

$$(i) a_n \not\equiv 0 \pmod{p} \Rightarrow p \nmid a_n.$$



(ii)  $a_i \equiv 0 \pmod{p} \quad \forall i < n \Rightarrow p \mid a_i \quad \forall i < n$ .

(iii)  $a_0 \not\equiv 0 \pmod{p^2} \Rightarrow p^2 \nmid a_0$ .

Then,  $f(x)$  is irreducible over  $\mathbb{Q}$ .

□ proof:

we need to show that  $f(x)$  doesn't factor into polynomials of lower degree in  $\mathbb{K}[x]$ .

Let  $f(x) = (b_r x^r + \dots + b_0)(c_s x^s + \dots + c_0)$  be a factorization of  $f(x)$  in  $\mathbb{K}[x]$  with  $b_r \neq 0$ ,  $c_s \neq 0$  and  $r < n$ ,  $s < n$ .

$\therefore a_0 \not\equiv 0 \pmod{p^2}$

$\therefore$  not both  $b_0$  and  $c_0$  are congruent to 0 modulo  $p$ .

Suppose that  $b_0 \not\equiv 0 \pmod{p}$  and  $c_0 \equiv 0 \pmod{p}$ .

$\therefore a_n \not\equiv 0 \pmod{p}$

$\therefore b_r \not\equiv 0 \pmod{p}$  and  $c_s \not\equiv 0 \pmod{p}$  (because  $a_n \equiv b_r c_s$ ).

Let  $m$  be the smallest value of  $k$  such that  $c_k \not\equiv 0 \pmod{p}$ .

Then,  $a_m = b_0 c_m + b_1 c_{m-1} + \dots + b_{m-i} c_i$  for some  $i$ ,  $0 \leq i < m$ .

Now  $b_0$  and  $c_m$  neither congruent to 0 modulo  $p$  and  $c_{m-1}, \dots, c_i$  all congruent to 0 modulo  $p$ .

$\Rightarrow a_m \not\equiv 0 \pmod{p}$

So,  $m = n \Rightarrow s = n$  which is contradiction to our assumption that  $s < n$ .

$\therefore f(x)$  is irreducible over  $\mathbb{Q}$ .



### ➤ Example :

(1) The polynomial  $f(x) = 25x^5 - 9x^4 + 3x^2 - 12$  is irreducible over  $\mathbb{Q}$ , because;

$\exists$  prime number  $p = 3 \exists$

(i)  $p \nmid 25$ .

(ii)  $p \mid -9$ ,  $p \mid 3$ ,  $p \mid -12$

(iii)  $p^2 \nmid -12$

Hence, from Eisenstein's theorem  $\Rightarrow f(x)$  is irreducible

(2) The polynomial  $f(x) = x^2 - 2 \in \mathbb{Q}[x]$  is irreducible over  $\mathbb{Q}$  because;

$\exists$   $p$  prime number,  $p = 2 \exists$

(i)  $p \nmid 1$ .

(ii)  $p \mid 0$  and  $p \mid -2$ .

(iii)  $p^2 \nmid -2$ .

$\therefore f(x)$  is irreducible over  $\mathbb{Q}$ .

### ◆ Remark :

The polynomial  $f(x) = x^{p-1} + x^{p-2} + \dots + x + 1$  is irreducible over  $\mathbb{Q} \forall p$  where  $p$  is a prime number.

### ▣ proof :

The previous polynomial is a cyclotomic polynomial can be given of the form :



$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \dots + x + 1$$

Let  $g(x) = \Phi_p(x+1)$

$$\Rightarrow g(x) = \frac{(x+1)^p - 1}{(x+1) - x} = x^p + \binom{p}{1}x^{p-1} + \dots + px$$

$$\Rightarrow g(x) = x^{p-1} + \binom{p}{1}x^{p-2} + \dots + p$$

we find that  $g(x)$  satisfies the conditions of Eisenstein's theorem for the prime number  $p$ .

$\therefore g(x)$  is irreducible over  $\mathbb{Q}$ .

So, if  $\Phi_p(x) = h(x)r(x)$  is a nontrivial factorisation of  $\Phi_p(x)$  in  $\mathbb{Q}[x]$ , then  $\Phi_p(x+1) = g(x) = h(x+1)r(x+1)$  would give a nontrivial factorisation of  $g(x)$  in  $\mathbb{Q}[x]$  which is not satisfied.

$\therefore \Phi_p(x)$  must be irreducible over  $\mathbb{Q}$ .

## (2) Ideal structure in $F[x]$

I. Definition: (principal ideal)

Let  $R$  be a commutative ring with unity and  $a \in R$ .

The ideal  $\{ra \mid r \in R\}$  of all multiples of  $a$  is the principal ideal generated by  $a$  and is denoted by  $\langle a \rangle$ .

An ideal  $N$  of  $R$  is a principal ideal if  $N = \langle a \rangle$  for some  $a \in R$ .



### Example :

The ideal  $\langle x \rangle$  is a principal ideal consists of all polynomials in  $F[x]$  having zero constant term.

### II. Theorem (1) :

If  $F$  is a field, then every ideal in  $F[x]$  is principal (i.e.  $F[x]$  is a principal ideal domain).

### Proof :

Let  $F$  be a field.

Suppose that  $N$  is an ideal of  $F[x]$ .

(i) If  $N = \{0\}$ , then  $N = \langle 0 \rangle$  (i.e.  $N = \langle 0 \rangle$  is a principal ideal).

(ii) If  $N \neq \{0\}$  and  $g(x)$  is a non-zero element of  $N$  of minimal degree, then the degree of  $g(x)$  is zero, hence  $g(x)$  is a unit, so  $N = \langle 1 \rangle = F[x]$  is a principal ideal.

(iii) If  $\deg[g(x)] \geq 1$ , then;

Let  $f(x)$  be any element of  $N$ .

By division algorithm theorem:

$$f(x) = g(x)q(x) + r(x) \text{ such that } \deg[r(x)] < \deg[g(x)]$$

$$\therefore f(x) \in N \text{ and } g(x) \in N$$

$$\therefore r(x) \in N \text{ because } r(x) = f(x) - g(x)q(x) \text{ (Definition of an ideal).}$$



Since,  $g(x)$  is a nonzero element of minimal degree in  $N$  (which is  $\neq 0$ ), then we must have  $r(x) = 0$ .  
Thus,  $f(x) = g(x)q(x)$  and  $N = \langle g(x) \rangle \neq$

### III. Theorem (2):

An ideal  $\langle p(x) \rangle \neq \{0\}$  of  $F[x]$  is maximal if and only if  $p(x)$  is irreducible over  $F$ .

▣ proof :

Let  $F$  be a field.

i) proving that :

$\{0\} \neq \langle p(x) \rangle \triangleleft F[x]$ ,  $\langle p(x) \rangle$  is maximal  $\Rightarrow p(x)$  is irreducible over  $F$ .

Let  $\langle p(x) \rangle \neq \{0\}$  be a maximal ideal of  $F[x]$ .

$\therefore \langle p(x) \rangle$  is maximal.

$\therefore \langle p(x) \rangle \neq F[x]$

$\Rightarrow p(x) \notin F$  (i.e.  $p(x)$  isn't of degree zero)

Let  $p(x) = f(x)g(x)$  be a factorization of  $p(x)$  in  $F[x]$ .

$\therefore \langle p(x) \rangle$  is a maximal ideal.

$\therefore \langle p(x) \rangle$  is a prime ideal. (Theorem which states that "For a commutative ring with unity  $R$ , if  $M$  is a maximal ideal of  $R$ , then  $M$  is a prime ideal of  $R$ ")

$\therefore \langle p(x) \rangle$  is a prime ideal,  $p(x) = f(x)g(x)$ ,  $p(x) \in \langle p(x) \rangle$

$\therefore f(x) \in \langle p(x) \rangle$  or  $g(x) \in \langle p(x) \rangle$

$\Rightarrow \exists q_1(x), q_2(x) \in F[x] \ni g(x) = p(x)q_1(x)$  or  $f(x) = p(x)q_2(x)$



$\Rightarrow \deg[g(x)] > \deg[p(x)]$  or  $\deg[f(x)] > \deg[p(x)]$   
which is contradiction to the factorization assumption.  
 $\therefore p(x)$  is irreducible over  $F$ .

ii) proving that:

$p(x)$  is irreducible over  $F \Rightarrow \langle p(x) \rangle$  is maximal.  
Let  $p(x)$  be an irreducible polynomial over  $F$ .

Suppose that  $I$  is an ideal of  $F[x]$  such that:

$$N = \langle p(x) \rangle \subseteq I \subseteq F[x]$$

$\Rightarrow I$  is a principal ideal of  $F[x]$  (II. Theorem (1))

$\Rightarrow \exists h(x) \in F[x] \ni I = \langle h(x) \rangle$

$$\therefore \langle p(x) \rangle \subseteq \langle h(x) \rangle \subseteq F[x]$$

$$\therefore p(x) \in \langle h(x) \rangle \quad (\text{because } \langle p(x) \rangle \subseteq \langle h(x) \rangle)$$

$\Rightarrow \exists q(x) \in F[x] \ni p(x) = h(x)q(x)$

But  $p(x)$  is irreducible, hence either  $h(x)$  or  $q(x)$  is of degree 0.

i) If  $\deg[h(x)] = 0$ , then  $h(x)$  is a non-zero constant in  $F$  which implies that  $h(x)$  is a unit in  $F[x]$ .

$$\text{So, } \langle h(x) \rangle = F[x] \Rightarrow I = F[x].$$

ii) If  $\deg[q(x)] = 0$ , then  $q(x)$  is a non-zero constant in  $F$  which implies that  $q(x)$  is a unit in  $F[x]$ .

$$\text{i.e. } q(x) = c.$$

$$\therefore p(x) = h(x)q(x) \quad \therefore p(x) = c h(x)$$

$$\Rightarrow h(x) = \frac{1}{c} p(x) \in \langle p(x) \rangle$$

$$\Rightarrow \langle h(x) \rangle = \langle \frac{1}{c} p(x) \rangle = N.$$

$$\therefore I = N$$

$$\therefore N = \langle p(x) \rangle \text{ is maximal.}$$



### Example :

Is  $\mathbb{F}_5[x]/\langle x^3 + 3x + 2 \rangle$  is a field ?!

Let  $p(x) = x^3 + 3x + 2$

$\mathbb{F}_5[x]/\langle p(x) \rangle$  is a field  $\iff \langle p(x) \rangle$  is maximal.

(Theorem)

$\langle p(x) \rangle$  is maximal  $\iff p(x)$  is irreducible over  $\mathbb{F}_5$ .

(Theorem)

Hence, to prove that  $\mathbb{F}_5[x]/\langle p(x) \rangle$  is a field all we need to do is to prove that  $p(x)$  is irreducible over  $\mathbb{F}_5$ .

To prove that  $p(x)$  is irreducible over  $\mathbb{F}_5$ , only we need to show that it has no zeroes in  $\mathbb{F}_5$ .

$$\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$$

$$p(0) = (0)^3 + 3(0) + 2 = 2 \neq 0$$

$$p(1) = (1)^3 + 3(1) + 2 = 6 = 1 \neq 0$$

$$p(2) = (2)^3 + 3(2) + 2 = 16 = 1 \neq 0$$

$$p(3) = (3)^3 + 3(3) + 2 = 38 = 3 \neq 0$$

$$p(4) = (4)^3 + 3(4) + 2 = 78 = 3 \neq 0$$

$\therefore p(x)$  has no zeroes in  $\mathbb{F}_5$

$\therefore p(x)$  is irreducible over  $\mathbb{F}_5$ .

$\therefore \mathbb{F}_5[x]/\langle p(x) \rangle$  is a field  $\neq$



\* Day: Tuesday

\* Subject: Abstract algebra (3)

\* Date:

\* Lecture: 5

## (1) Application to unique factorization in $F[x]$

### I. Theorem (1):

Let  $p(x)$  be an irreducible polynomial in  $F[x]$ .

If  $p(x)$  divides  $r(x)s(x)$  for  $r(x), s(x) \in F[x]$ , then either  $p(x)$  divides  $r(x)$  or  $p(x)$  divides  $s(x)$ .

□ proof:

Let  $F$  be a field and  $p(x) \in F[x]$

Suppose that  $p(x)$  is irreducible over  $F$ .

Let  $p(x)$  divides  $r(x)s(x)$ ;  $r(x), s(x) \in F[x]$ .

$\therefore p(x)$  is irreducible over  $F$ .

$\therefore \langle p(x) \rangle$  is a maximal ideal of  $F[x]$ .

$\therefore p(x)$  divides  $r(x)s(x)$ .

$\therefore r(x)s(x) \in \langle p(x) \rangle$  (because  $r(x)s(x)$  is a multiple of  $p(x)$ ).

$\therefore \langle p(x) \rangle$  is a maximal ideal of  $F[x]$ .

$\therefore \langle p(x) \rangle$  is a prime ideal of  $F[x]$ . (theorem).

$\therefore r(x)s(x) \in \langle p(x) \rangle$

$\therefore r(x) \in \langle p(x) \rangle$  or  $s(x) \in \langle p(x) \rangle$

$\Rightarrow \exists q_1(x), q_2(x) \in F[x] \ni r(x) = q_1(x)p(x)$  or  $s(x) = q_2(x)p(x)$

$\therefore p(x)$  divides  $r(x)$  or  $p(x)$  divides  $s(x)$ .



## II. Theorem (2):

If  $F$  is a field, then every nonconstant polynomial  $f(x) \in F[x]$  can be factored in  $F[x]$  into a product of irreducible polynomials, the irreducible polynomials being unique except for order and for unit factors in  $F$ .

### Proof:

Let  $f(x) \in F[x]$  be a nonconstant polynomial.

Then  $f(x)$  has two cases: reducible or irreducible.

(1) In case of  $f(x)$  is irreducible:

proof ends.

(2) In case of  $f(x)$  is reducible:

Let  $f(x) = g(x)h(x)$ ,  $\deg[g(x)] < \deg[f(x)]$  and  $\deg[h(x)] < \deg[f(x)]$ .

In this case we have other two cases:

(i)  $g(x)$  and  $h(x)$  both are irreducible:

proof ends.

(ii) At least one of  $g(x)$  and  $h(x)$  factors into polynomials of lower degree, say  $g(x)$ .

$\Rightarrow g(x) = p_1(x)p_2(x)$ ,  $\deg[p_1(x)]$  and  $\deg[p_2(x)] < \deg[g(x)]$ .

$\Rightarrow f(x) = p_1(x)p_2(x)h(x)$

Continuing this process we arrive at a factorization:

$$f(x) = p_1(x)p_2(x) \cdots p_r(x)$$

where  $p_i(x)$  is irreducible for  $1 \leq i \leq r$ .

It remains to show uniqueness:



Suppose that:

$$f(x) = p_1(x) p_2(x) \dots p_r(x) = q_1(x) q_2(x) \dots q_s(x)$$

are two factorizations of  $f(x)$  into irreducible polynomials.

Then using the Corollary which states that "If  $p(x)$  is irreducible in  $F[x]$  and  $p(x)$  divides the product  $r_1(x) \dots r_n(x)$  for  $r_i(x) \in F[x]$ , then  $p(x)$  divides  $r_i(x)$  for at least one  $i$ ". Hence,  $p_1(x)$  divides some  $q_j(x)$ , say  $q_1(x)$ .

But  $q_1(x)$  is irreducible.

then,  $q_1(x) = u_1 p_1(x)$  where  $u_1 \neq 0$  is a unit in  $F$ .

Substituting  $u_1 p_1(x)$  for  $q_1(x)$ , we get:

$$p_1(x) p_2(x) \dots p_r(x) = u_1 p_1(x) q_2(x) \dots q_s(x)$$

$$\Rightarrow p_2(x) \dots p_r(x) = u_1 q_2(x) \dots q_s(x)$$

By a similar argument, say  $q_2(x) = u_2 p_2(x)$

$$\Rightarrow p_2(x) p_3(x) \dots p_r(x) = u_1 u_2 p_2(x) q_3(x) \dots q_s(x)$$

$$\Rightarrow p_3(x) \dots p_r(x) = u_1 u_2 q_3(x) \dots q_s(x)$$

Continuing in this manner, we eventually arrive at:

$$1 = u_1 u_2 \dots u_r \frac{q_1(x) \dots q_s(x)}{p_1(x) \dots p_r(x)}$$

But this equation is possible only if  $s = r$

$$\Rightarrow 1 = u_1 u_2 \dots u_r$$

Thus, the irreducible factors  $p_i(x)$  and  $q_j(x)$  were the same except for order and unit factors.

### Example:

Show that the factorization of  $f(x) = x^4 + 3x^3 + 2x + 4$  in  $\mathbb{K}_5[x]$  is  $(x-1)^3(x+1)$  and these irreducible factors in  $\mathbb{K}_5[x]$  are only defined up to units in  $\mathbb{K}_5[x]$ .



$$K_5 = \{0, 1, 2, 3, 4\}$$

$$f(x) = x^4 + 3x^3 + 2x + 4$$

$$f(0) = (0)^4 + 3(0)^3 + 2(0) + 4 = 4 \neq 0$$

$$f(1) = (1)^4 + 3(1)^3 + 2(1) + 4 = 10 \neq 0$$

$\therefore 1 \in K_5$  is a zero of  $f(x)$

$\Rightarrow (x-1)$  is a factor of  $f(x)$

using division algorithm, we arrive at

$$\begin{array}{r} x^3 + 4x^2 + 4x + 1 \\ (x-1) \overline{) x^4 + 3x^3 + 2x + 4} \\ \underline{x^4 - x^3} \end{array}$$

$$4x^3 + 2x + 4$$

$$4x^3 - 4x^2$$

$$4x^2 + 2x + 4$$

$$4x^2 - 4x$$

$$1x + 4$$

$$x - 1$$

$$5 = 0$$

$$\therefore f(x) = (x-1)(x^3 + 4x^2 + 4x + 1)$$

and by repeating the division we get:

$$f(x) = (x-1)(x-1)(x-1)(x+1) = (x-1)^3(x+1)$$

$$= (x-1)(x+1)(x-1)(x-1)$$

$$= (2x-2)(3x+3)(x-1)(x-1) \text{ and so on.}$$



## (2) Rings of endomorphisms

### I. Definition:

Let  $A$  be an abelian group.

A homomorphism of  $A$  into itself is an endomorphism.

### II. Theorem:

The set  $\text{Hom}(A)$  of all endomorphisms of an abelian group  $A$  forms a ring under homomorphism addition and homomorphism multiplication (homomorphism composition).

### ◆ Remark:

(1) The set  $\text{Hom}(A) = \{f: A \rightarrow A \mid f \text{ is a homomorphism}\}$

(2) Homomorphism addition is defined as:

$$(\phi + \psi)(a) = \phi(a) + \psi(a) \quad \forall \phi, \psi \in \text{Hom}(A)$$

(3) Homomorphism multiplication is defined as:

$$(\phi \psi)(a) = \phi(a) \psi(a) \quad \forall \phi, \psi \in \text{Hom}(A)$$

### ■ proof:

(i)  $\forall \phi, \psi \in \text{Hom}(A)$  where

$$\phi: A \xrightarrow{\text{hom.}} A$$

$$\psi: A \xrightarrow{\text{hom.}} A$$

$$(\phi + \psi)(a+b) = \phi(a+b) + \psi(a+b)$$



$$= \phi(a) + \phi(b) + \psi(a) + \psi(b)$$

$$= [\phi(a) + \psi(a)] + [\phi(b) + \psi(b)]$$

$$= (\phi + \psi)(a) + (\phi + \psi)(b)$$

$$\therefore \phi + \psi : A \xrightarrow{\text{hom.}} A \Rightarrow \phi + \psi \in \text{Hom}(A).$$

$$(ii) \forall \phi, \psi, \theta \in \text{Hom}(A).$$

$$[(\phi + \psi) + \theta](a) = (\phi + \psi)(a) + \theta(a)$$

$$= \phi(a) + \psi(a) + \theta(a)$$

$$= \phi(a) + [\psi(a) + \theta(a)] = \phi(a) + (\psi + \theta)(a)$$

$$= [\phi + (\psi + \theta)](a).$$

$$\therefore (\phi + \psi) + \theta = \phi + (\psi + \theta).$$

$$(iii) \exists 0 \in \text{Hom}(A) \text{ defined as } [0(a) = e], e \text{ is identity of } A.$$

$$\forall \phi \in \text{Hom}(A) \Rightarrow (0 + \phi)(a) = (\phi + 0)(a) = \phi(a).$$

because ;

$$(0 + \phi)(a) = 0(a) + \phi(a) = e + \phi(a) = \phi(a)$$

$$(\phi + 0)(a) = \phi(a) + 0(a) = \phi(a) + e = \phi(a).$$

$$(iv) \forall \phi \in \text{Hom}(A) \exists -\phi \in \text{Hom}(A) \text{ defined as}$$

$$(-\phi)(a) = -\phi(a)$$

$$\text{Hence ; } [\phi + (-\phi)](a) = \phi(a) + (-\phi)(a)$$

$$= \phi(a) - \phi(a) = 0 = [(-\phi) + \phi](a).$$

$$(v) \forall \phi, \psi \in \text{Hom}(A)$$

$$(\phi + \psi)(a) = \phi(a) + \psi(a) = \psi(a) + \phi(a) = (\psi + \phi)(a).$$

$$(vi) \forall \phi, \psi \in \text{Hom}(A).$$

$$(\psi\phi)(ab) = (\psi\phi)(a) \cdot (\psi\phi)(b)$$

$$= \psi(a)\phi(a) \cdot \psi(b)\phi(b)$$

$$= \psi(ab) \cdot \phi(ab)$$

$$= \psi(a)\psi(b) \cdot \phi(a)\phi(b)$$

$$= (\psi(a)\phi(a))(\psi(b)\phi(b))$$



$$= (\psi\phi)(a) \cdot (\psi\phi)(b)$$

$$\therefore \psi\phi : A \xrightarrow{\text{hom.}} A \Rightarrow \psi\phi \in \text{Hom}(A)$$

(vi) let  $\psi, \phi, \theta \in \text{Hom}(A)$ .

$$\begin{aligned} ((\psi\phi)\theta)(a) &= (\psi\phi)(a) \cdot \theta(a) \\ &= \psi(a) \phi(a) \theta(a) \\ &= \psi(a) (\phi(a) \theta(a)) \\ &= \psi(a) [(\phi\theta)(a)] \\ &= (\psi(\phi\theta))(a) \end{aligned}$$

$$\therefore (\psi\phi)\theta = \psi(\phi\theta)$$

(viii) let  $\psi, \phi, \theta \in \text{Hom}(A)$  and  $a \in A$ .

$$\begin{aligned} [\theta(\phi + \psi)](a) &= (\theta(a))((\phi + \psi)(a)) \\ &= \theta(a) [\phi(a) + \psi(a)] \\ &= \theta(a)\phi(a) + \theta(a)\psi(a) \\ &= (\theta\phi + \theta\psi)(a) \end{aligned}$$

$$\therefore \theta(\phi + \psi) = \theta\phi + \theta\psi$$

$$\begin{aligned} \text{Similarly; } [(\psi + \theta)\phi](a) &= (\psi + \theta)(a) \cdot \phi(a) \\ &= [\psi(a) + \theta(a)] \phi(a) = \psi(a)\phi(a) + \theta(a)\phi(a) \\ &= (\psi\phi + \theta\phi)(a) \end{aligned}$$

$$\therefore (\psi + \theta)\phi = \psi\phi + \theta\phi \quad \neq$$

➤ Example:

Consider the abelian group  $(\mathbb{Z} \times \mathbb{Z}, +)$ .

We can specify an endomorphism of this group by giving its values on the generators  $(1,0)$  and  $(0,1)$  of the group.

Define  $\phi \in \text{Hom}[(\mathbb{Z} \times \mathbb{Z}, +)]$  by:

$$\phi(1,0) = (1,0) \quad \text{and} \quad \phi(0,1) = (1,0)$$



Define  $\psi$  by:

$$\psi(1,0) = (0,0) \text{ and } \psi(0,1) = (0,1)$$

we can find that:

$$\phi(n,m) = (n+m, 0)$$

$$\psi(n,m) = (0,m)$$

we need to prove that  $\psi \circ \phi \neq \phi \circ \psi$ .

$$(\psi \circ \phi)(n,m) = \psi[\phi(n,m)] = \psi(n+m, 0) = (0,0)$$

$$(\phi \circ \psi)(n,m) = \phi[\psi(n,m)] = \phi(0,m) = (m,0)$$

$$\therefore \phi \circ \psi \neq \psi \circ \phi.$$

### (3) Factorization

I. Definition (1): (factor)

Let  $D$  be an integral domain and  $a, b \in D$ .

If there exists  $c \in D$  such that  $b = ac$ , then  $a$  divides  $b$  (or  $a$  is a factor of  $b$ ) denoted by  $a|b$ .

II. Definition (2): (unit, associates)

An element  $u$  of an integral domain  $D$  is a unit of  $D$  if  $u$  divides  $1$ .

$$\text{i.e.: } u|1 \equiv \exists v \in D \ni u \cdot v = 1.$$

Two elements  $a, b \in D$  are associates in  $D$  if  $a = bu$  where  $u$  is a unit in  $D$ .

$$\text{i.e.: } a \sim b \text{ if } \exists u \in D \ni a = ub \text{ and } \exists v \in D \ni b = va.$$



## III. Definition (3): (Irreducible)

A non-zero element  $p$  that's not a unit of an integral domain  $D$  is an irreducible of  $D$  if in any factorization  $p = ab$  in  $D$  either  $a$  or  $b$  is a unit.

## IV. Definition (4): (U.F.D.)

An integral domain  $D$  is a unique factorization domain (abbreviated UFD) if the following conditions are satisfied:

- 1) Every element of  $D$  that's neither 0 nor a unit can be factored into a product of a finite number of irreducibles.
- 2) If  $p_1 p_2 \dots p_r$  and  $q_1 q_2 \dots q_s$  are two factorizations of the same element of  $D$  into irreducibles, then  $r = s$  and  $q_j$  can be renumbered so that  $p_i$  and  $q_j$  are associates.



⊗ Day: Tuesday  
⊗ Subject: Abstract algebra (3)

⊗ Date: 31/3/2015  
⊗ Lecture: 6

## [1] Remark

### I. Factor :

$D$  - I.D. ,  $a, b \in D$ .

$$a \mid b \iff \exists c \in D \ni b = ac$$

for example:

in  $\mathbb{Z}$  ;  $3 \mid 6$  because  $\exists 2 \in \mathbb{Z} \ni 6 = 3 \cdot 2$

### II. Unit :

$D$  - I.D. ,  $u \in D$ .

$$u \text{ is a unit} \iff u \mid 1 \iff \exists v \in D \ni uv = 1$$

for example:

in  $\mathbb{Z}$  ; units are 1 and -1 i.e.  $U = \{1, -1\}$

where  $U$  is the set of all units in  $\mathbb{Z}$ .

### III. Associates :

$D$  - I.D. ,  $a, b \in D$ .

$$a \sim b \iff \exists u \in D \ni a = bu \text{ where } u \text{ is a unit.}$$

for example:

in  $\mathbb{Z}$  ;  $5 \sim -5$  because  $5 = (-5)(-1)$  ;  $(-1)$  is a unit

and generally  $x \sim -x \quad \forall x \in \mathbb{Z}$ .

In  $\mathbb{C}$  ;  $U = \{1, -1, i, -i\} \implies 5 \sim 5i$



## IV. Irreducible :

$D$  - I.D. ,  $p \in D$ .

$p$  is an irreducible element  $\Leftrightarrow$  if  $p = ab \Rightarrow a$  is a unit or  $b$  is a unit.

for example :

In  $\mathbb{Z}$  ; 5 is irreducible because  $5 = 5 \cdot 1$  ,  
1 is a unit.

## [2] Theorem (1)

### I. Theorem (I) :

Every principal ideal domain (PID) is a unique factorization domain (UFD). (but not vice versa)

i.e.  $D$  - PID  $\Rightarrow$   $D$  - UFD.

### II. Theorem (II) :

If  $D$  is a unique factorization domain (UFD), then  $D[x]$  is a unique factorization domain.

i.e.  $D$  - UFD  $\Rightarrow$   $D[x]$  - UFD

### III. Remark :

- (1) Every field is a unique factorization domain.
- (2) if  $F$  is a field, then  $F[x]$  is a (UFD).



□ proof:

Let  $F$  be a field.

∴ every field is an integral domain.

∴  $F$  is an integral domain.

∴ every field is a principal ideal domain (theorem) ×

∴  $F$  is a principal ideal domain.

using the previous theorem "Every (PID) is a (UFD)"

∴  $F$  is a unique factorization domain.

using the second theorem " $D: \text{UFD} \Rightarrow D[x] = \text{UFD}$ "

∴  $F[x]$  is a unique factorization domain.

▷ Example:

$\mathbb{K}$  is a principal ideal domain  $\Rightarrow \mathbb{K}$  is a unique factorization domain  $\Rightarrow \mathbb{K}[x]$  is a unique factorization domain.

### [5] Lemma (1)

I. Lemma: (Ascending Chain condition for a (PID))

Let  $D$  be a principal ideal domain.

If  $N_1 \subseteq N_2 \subseteq \dots$  is a monotonic ascending chain of ideals  $N_i$ .

Then there exists a positive integer  $r$  such that  $N_r = N_s$  for all  $s \geq r$ .



□ proof:

Let  $D$  be a principal ideal domain.

Suppose that  $N_1 \subseteq N_2 \subseteq N_3 \subseteq \dots$  is a monotonic ascending chain of ideals  $N_i$  in  $D$ .

Let  $N = \bigcup_i N_i$ ,  $N_i \triangleleft D \forall i$ .

Now, we need to prove that  $N$  is an ideal of  $D$ .

$\therefore N = \bigcup_i N_i$ ,  $N_i \triangleleft D \forall i$ .

$\therefore N \subseteq D$ .

Let  $a, b \in N$ .

$\Rightarrow \exists i, j \in \mathbb{N}^+ \ni a \in N_i, b \in N_j$ .

Now, either  $N_i \subseteq N_j$  or  $N_j \subseteq N_i$ .

Suppose that  $N_i \subseteq N_j$ .

$\therefore a, b \in N_j$

$\therefore N_j \triangleleft D$ .

$\therefore a + b \in N_j$ ,  $N_j \subseteq N$ .

$\therefore a + b \in N$ .  $\rightarrow (1)$

$\forall a \in N, d \in D \Rightarrow a \in N_i$  for some  $i$ .

$\therefore N_i$  is an ideal of  $D$ .

$\therefore ad \in N_i$  and  $da \in N_i$ .

$\therefore N_i \subseteq N$

$\therefore ad \in N$  and  $da \in N$ .  $\rightarrow (2)$

From (1) and (2):

$\therefore N$  is an ideal of  $D$  ( $N \triangleleft D$ ).

$\therefore D$  is a principal ideal domain.

$\therefore N = \langle c \rangle$  for some  $c \in D$ .

$\therefore N = \bigcup_i N_i \quad \therefore \exists r \in \mathbb{N}^+ \ni c \in N_r$



for  $S \geq r$  we have

$$\langle c \rangle = N_r \subseteq N_S \subseteq N = \langle c \rangle$$

$$\therefore N_r = N_S \quad \forall S \geq r. \quad \#$$

II. Remark:

Let  $D$  be a principal ideal domain.

Suppose that  $a, b \in D$ , then:

(i)  $\langle a \rangle \subseteq \langle b \rangle \iff b \mid a$ .

(ii)  $\langle a \rangle = \langle b \rangle \iff a \sim b$ .

(iii)  $\langle a \rangle = \{ra \mid r \in D\}$

(iv)  $a \sim b \iff a \mid b$  and  $b \mid a$ .

□ proof:

(i)  $\langle a \rangle \subseteq \langle b \rangle \iff b \mid a$ .

Let  $D$  be a principal ideal domain and  $a, b \in D$ .

(1) proving that:

$$\langle a \rangle \subseteq \langle b \rangle \implies b \mid a.$$

$$\text{Let } \langle a \rangle \subseteq \langle b \rangle.$$

$$\therefore a \in \langle a \rangle, \langle a \rangle \subseteq \langle b \rangle.$$

$$\therefore a \in \langle b \rangle.$$

$$\implies \exists c \in D \exists a = bc$$

$$\therefore b \mid a \quad \#$$

(2) proving that:

$$b \mid a \implies \langle a \rangle \subseteq \langle b \rangle.$$

$$\therefore b \mid a$$

$$\therefore \exists c \in D \exists a = bc \rightarrow \oplus$$



To prove that  $\langle a \rangle \subseteq \langle b \rangle$ , then we need to prove that

$$\forall x \in \langle a \rangle \Rightarrow x \in \langle b \rangle$$

Let  $x \in \langle a \rangle$ .

$$\Rightarrow \exists y \in D \ni x = ay.$$

$$\text{But from } \oplus \Rightarrow x = ay = b(cy).$$

$$\therefore b \mid x \quad \forall x \in \langle a \rangle.$$

$$\Rightarrow x \in \langle b \rangle \quad \forall x \in \langle a \rangle.$$

$$\therefore \langle a \rangle \subseteq \langle b \rangle. \quad \#$$

$$(ii) \quad \langle a \rangle = \langle b \rangle \Leftrightarrow a \sim b.$$

Let  $D$  be a principal ideal domain and  $a, b \in D$ .

(1) proving that:

$$\langle a \rangle = \langle b \rangle \Rightarrow a \sim b.$$

$$\text{Let } \langle a \rangle = \langle b \rangle.$$

$$\therefore \langle a \rangle = \langle b \rangle$$

$$\therefore \langle a \rangle \subseteq \langle b \rangle \quad \text{and} \quad \langle b \rangle \subseteq \langle a \rangle$$

$$\Rightarrow b \mid a \quad \text{and} \quad a \mid b$$

$$\therefore a \sim b.$$

(2) proving that:

$$a \sim b \Rightarrow \langle a \rangle = \langle b \rangle.$$

$$\text{Let } a \sim b.$$

$$\therefore a \sim b.$$

$$\therefore a \mid b \quad \text{and} \quad b \mid a.$$

$$\Rightarrow \exists u, u' \in D \ni b = au \quad \text{and} \quad a = bu'$$

$$\Rightarrow \langle a \rangle \subseteq \langle b \rangle \quad \text{and} \quad \langle b \rangle \subseteq \langle a \rangle.$$

$$\therefore \langle a \rangle = \langle b \rangle$$



(iv)  $a \sim b \iff a|b$  and  $b|a$ .

Let  $D$  be an ~~an principal ideal domain~~ integral domain and  $a, b \in D$ .

(1) proving that:

$$a \sim b \implies a|b \text{ and } b|a.$$

Let  $a \sim b$ .

$$\therefore a \sim b$$

$$\therefore \exists u \in D \exists a = bu \text{ where } u \text{ is a unit in } D.$$

$$\implies b|a.$$

$\therefore u$  is a unit in  $D$ .

$$\therefore \exists v \in D \exists uv = 1.$$

$\therefore a = bu$ ,  $D$  is an integral domain.

$$\therefore a \cdot v = bu \cdot v$$

$$\therefore uv = 1$$

$$\therefore b = av, \text{ } v \text{ is a unit.}$$

$$\implies a|b.$$

(2) proving that:

$$a|b \text{ and } b|a \implies a \sim b.$$

Let  $a|b$  and  $b|a$ .

$$\implies b = ua \text{ and } a = vb.$$

$$\implies a = vb = v(ua) \implies a = vua \implies vu = 1$$

$\therefore u$  and  $v$  are units.

Hence,  $a \sim b$ .

### [4] Theorem (2)

Let  $D$  be a principal ideal domain (PID).



Every element that's neither 0 nor a unit in  $D$  is a product of irreducibles.

□ proof:

Let  $D$  be a principal ideal domain.

Suppose that  $a \in D$  where  $a$  is neither 0 nor a unit.  
If  $a$  is irreducible, then the proof ends.

If  $a$  is reducible, then:

$\exists a_1, b_1 \in D \ni a = a_1 b_1$ ,  $a_1, b_1$  aren't units.

$\dots a = a_1 b_1 \Rightarrow a_1 \mid a \Rightarrow \langle a \rangle \subset \langle a_1 \rangle$ .

If  $a_1$  is reducible, then:

$\exists a_2, b_2 \in D \ni a_1 = a_2 b_2$ ,  $a_2, b_2$  aren't units.

$\dots a_1 = a_2 b_2 \Rightarrow a_2 \mid a_1 \Rightarrow \langle a_1 \rangle \subset \langle a_2 \rangle$

Continuing this procedure, we arrive at,

$\langle a \rangle \subset \langle a_1 \rangle \subset \langle a_2 \rangle \subset \dots$

By the ACC Lemma, this chain terminates with some  $\langle a_r \rangle$  and  $a_r$  must be irreducible.

Now,  $a$  has an irreducible factor  $a_r = p_1$ .

$\Rightarrow a = p_1 c_1$  for  $p_1$  an irreducible and  $c_1$  not a unit.

Similarly;

$\langle a \rangle \subset \langle c_1 \rangle \subset \langle c_2 \rangle \subset \dots$

this chain must terminate with some  $c_r = q_r$  that's an irreducible.

$\therefore a = p_1 p_2 \dots p_r q_r$ ,  $p_i$  is irreducible.



### [5] Lemma (2)

An ideal  $\langle p \rangle$  in a principal ideal domain is maximal if and only if  $p$  is an irreducible.

Proof:

Let  $D$  be a principal ideal domain.

(i) proving that:

$\langle p \rangle$  is maximal  $\Rightarrow p$  is an irreducible.

Let  $\langle p \rangle$  be a maximal ideal of  $D$ .

Suppose that  $p = ab$ ,  $a, b \in D$ .

$\Rightarrow a \mid p \Rightarrow \langle p \rangle \subseteq \langle a \rangle \subseteq D$ .

$\therefore \langle p \rangle$  is maximal.

$\therefore \langle p \rangle = \langle a \rangle$  or  $\langle a \rangle = D = \langle 1 \rangle$ .

If  $\langle p \rangle = \langle a \rangle$ , then  $a \sim p$

$\therefore b$  is a unit

If  $\langle a \rangle = \langle 1 \rangle = D$ , then  $a \sim 1$

$\therefore a$  is a unit.

$\Rightarrow p$  is irreducible.

(ii) proving that:

$p$  is irreducible  $\Rightarrow \langle p \rangle$  is maximal.

Let  $p$  be an irreducible element.

Suppose that:

$\exists \langle a \rangle \subsetneq D \ni \langle p \rangle \subseteq \langle a \rangle \subsetneq D$ .

we need to prove that  $\langle p \rangle = \langle a \rangle$  or  $\langle a \rangle = D$ .

$\therefore p \in \langle p \rangle$  and  $\langle p \rangle \subseteq \langle a \rangle$



$$\therefore p \in \langle a \rangle.$$

$$\Rightarrow \exists b \in D \exists p = ab.$$

$\therefore p$  is irreducible.

$\therefore a$  is a unit or  $b$  is a unit.

If  $a$  is a unit, then  $\langle a \rangle = D = \langle 1 \rangle$ .

If  $b$  is a unit, then  $p = a \Rightarrow \langle p \rangle = \langle a \rangle$ .

$\therefore \langle p \rangle$  is a ~~principal~~ maximal ideal.

### [5] Theorem (3)

Every principal ideal domain (PID) is a unique factorization domain (UFD).

□ proof:

Let  $D$  be a (PID).

using theorem (2) which states that "Every element that's neither 0 nor a unit in a (PID) is a product of irreducibles".

Hence, each  $a \in D$ , where  $a$  is neither 0 nor a unit has a factorization:

$$a = p_1 p_2 \cdots p_r$$

where  $p_i$  is irreducible  $\forall 1 \leq i \leq r$

Let  $a = q_1 q_2 \cdots q_s$  be another factorization of  $a$  into irreducibles.

$$\Rightarrow p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

$$\Rightarrow p_i \mid (q_1 q_2 \cdots q_s) \Rightarrow p_i \mid q_i \text{ for some } i \text{ (Corollary)}$$



By changing the order of  $q_i$  if necessary, we can assume that  $i = 1$ .

$$\Rightarrow p_1 \nmid q_1 \Rightarrow q_1 = p_1 u_1.$$

$\therefore p_1$  is an irreducible.

$\therefore u_1$  is a unit.

$\Rightarrow p_1$  and  $q_1$  are associates.

Now, we have;

$$p_1 p_2 \dots p_r = p_1 u_1 q_2 \dots q_s$$

By the cancellation law in  $D$ ;

$$\Rightarrow p_2 \dots p_r = u_1 q_2 \dots q_s$$

Continuing this process, we finally arrive at

$$1 = u_1 u_2 \dots u_r q_{r+1} \dots q_s$$

$\therefore q_j$  are irreducibles  $\forall j$ .

$$\therefore r = s.$$

$$\Rightarrow 1 = u_1 u_2 \dots u_r$$

$$\Rightarrow p_i = u_i q_i. \quad \#$$

## [6] Definition

I. Definition := (prime element).

A nonzero nonunit element  $p$  of an integral domain  $D$  with the property that  $p \mid ab$  implies either  $p \mid a$  or  $p \mid b$  is a prime.

i.e.

$$p \text{ is prime} \Leftrightarrow (p \mid ab \Rightarrow p \mid a \text{ or } p \mid b).$$



## II. Example :

Every prime element in an integral domain is an irreducible element.

□ proof :

Let  $D$  be an integral domain and  $p$  be a prime element in  $D$ .

Suppose that  $p = ab$ .

$\therefore 1 \in D$ .

$\therefore ab = p \cdot 1 \Rightarrow p \mid ab$

$\therefore p$  is prime.

$\therefore p \mid a$  or  $p \mid b$

$\Rightarrow p \sim a$  or  $p \sim b$ .

$\Rightarrow b$  is a unit or  $a$  is a unit.

$\therefore p$  is irreducible.

◇ Remark :

(1) If  $D$  is a UFD, then every prime in  $D$  is irreducible and ~~every~~ every irreducible is prime.

i.e.  $p$  is prime in  $D \iff p$  is irreducible in  $D$ .

(2) If  $D$  is an integral domain (ID), then not always every irreducible is a prime.

For example:

$$\mathbb{H}[\sqrt{3}i] = \{a + \sqrt{3}ib \mid a, b \in \mathbb{H}, i = \sqrt{-1}\}$$



we need to prove that  $\mathbb{H}[\sqrt{3}i]$  is an integral domain and to do this we first prove that it's a subring of  $\mathbb{C}$ .

let  $x, y \in \mathbb{H}[\sqrt{3}i]$  where

$$x = a_1 + \sqrt{3}ib_1 \quad \text{and} \quad y = a_2 + \sqrt{3}ib_2.$$

$$\begin{aligned} \text{(i)} \quad x - y &= (a_1 + \sqrt{3}ib_1) - (a_2 + \sqrt{3}ib_2) \\ &= (a_1 - a_2) + \sqrt{3}i(b_1 - b_2) \in \mathbb{H}[\sqrt{3}i]. \end{aligned}$$

$$\begin{aligned} \text{(ii)} \quad x \cdot y &= (a_1 + \sqrt{3}ib_1)(a_2 + \sqrt{3}ib_2) \\ &= a_1a_2 + \sqrt{3}ia_1b_2 + \sqrt{3}ib_1a_2 + 3i^2b_1b_2 \\ &= (a_1a_2 - 3b_1b_2) + \sqrt{3}i(a_1b_2 + a_2b_1) \in \mathbb{H}[\sqrt{3}i]. \end{aligned}$$

$\therefore \mathbb{H}[\sqrt{3}i]$  is an integral domain.

let  $A = \mathbb{H}[\sqrt{3}i]$ .

we find that  $2 \in A$  and 2 is irreducible but not prime.  
To prove that;

$$\text{let } 2 = \alpha\beta, \quad \alpha, \beta \in A.$$

$$\Rightarrow 2 = (a + \sqrt{3}ib)(c + \sqrt{3}id), \quad a, b, c, d \in \mathbb{H}$$

⊕ Remark:

$$N(\alpha) = \alpha\bar{\alpha} = (a + \sqrt{3}ib)(a - \sqrt{3}ib) = a^2 + 3b^2$$

where  $N$  is the norm.

Hence, by taking norm for both sides,

$$N(2) = N(\alpha)N(\beta) \quad \text{because } N(\alpha\beta) = N(\alpha)N(\beta)$$

$$\Rightarrow 4 = (a^2 + 3b^2)(c^2 + 3d^2)$$

$$\Rightarrow (a^2 + 3b^2) = 1 \quad \text{and} \quad (c^2 + 3d^2) = 4. \quad \text{or}$$

$$(a^2 + 3b^2) = 4 \quad \text{and} \quad (c^2 + 3d^2) = 1.$$

$\therefore 2$  is irreducible.



$$4 = (1 + \sqrt{3}i)(1 - \sqrt{3}i) = 2 \cdot 2$$

$$2 \mid 4$$

$$2 \mid (1 + \sqrt{3}i) \text{ or } 2 \mid (1 - \sqrt{3}i)$$

$$1 + \sqrt{3}i = 2\alpha \text{ or } 1 - \sqrt{3}i = 2\beta$$

$$1 = 2\alpha \Rightarrow \alpha = \frac{1}{2} \notin \mathbb{K}, \text{ similarly } \beta = \frac{1}{2} \notin \mathbb{K}$$

2 not prime

## [7] primitive polynomial

Definition: (primitive polynomial)

Let  $D$  be a (UFD).

A nonconstant polynomial  $f(x)$ , where

$$f(x) = a_0 + a_1x + \dots + a_nx^n \in D[x]$$

is primitive if the only common divisors of all the  $a_i$  are units of  $D$ .

I. Example:

In  $\mathbb{K}[x]$ ;

1)  $f(x) = 4x^2 + 3x + 2$  is primitive.

2)  $g(x) = 4x^2 + 6x + 2$  isn't primitive because (2) which isn't a unit in  $\mathbb{K}$  is a common divisor of 4, 6 and 2.

II. Remark:

Every nonconstant irreducible polynomial in  $D[x]$  is



a primitive polynomial.

#### IV. Lemma (1):

If  $D$  is a UFD, then for every nonconstant polynomial  $f(x) \in D[x]$  we have  $f(x) = c g(x)$ , where  $c \in D$ ,  $g(x) \in D[x]$  and  $g(x)$  is primitive.

The element  $c$  is unique up to a unit factor in  $D$  and is the content of  $f(x)$ , also  $g(x)$  is unique up to a unit factor in  $D$ .

for example:

In  $\mathbb{K}[x]$ ;

$$4x^2 + 6x - 8 = 2(2x^2 + 3x - 4)$$

where  $2x^2 + 3x - 4$  is a primitive polynomial.

#### V. Lemma (2): (Gauss)

If  $D$  is a (UFD), then a product of two primitive polynomials in  $D[x]$  is again primitive.

#### VI. Lemma (3):

Let  $D$  be a (UFD) and let  $F$  be a field of quotients of  $D$ .

Let  $f(x) \in D[x]$ ,  $\deg[f(x)] > 0$ . If  $f(x)$  is an irreducible in  $D[x]$ , then  $f(x)$  is also an irreducible in  $F[x]$ . Also, if  $f(x)$  is primitive in  $D[x]$  and irreducible in  $F[x]$ , then  $f(x)$  is irreducible in  $D[x]$ .



\* Day: Tuesday

\* Subject: Abstract algebra

\* Date: 14/4/2015

\* Lecture: 7

## (1) Euclidean domains

### I. Definition (1): (Euclidean valuation)

An Euclidean valuation on an integral domain  $D$  is a function  $v$  mapping the nonzero elements of  $D$  into the nonnegative integers such that the following conditions are satisfied:

- (1)  $\forall a, b \in D, b \neq 0 \exists q, r \in D \ni a = bq + r$   
 $, r = 0 \text{ or } v(r) < v(b).$
- (2)  $\forall a, b \in D^* \Rightarrow v(a) \leq v(ab)$

i.e.  $v: D^* \longrightarrow \mathbb{N}^+ \cup \{0\}$   
where conditions (1) and (2) hold.

### II. Definition (2): (Euclidean domain)

An integral domain  $D$  is an Euclidean domain if there exists an Euclidean valuation on  $D$ .

### ➤ Examples:

- (1) The integral domain  $\mathbb{Z}$  is an Euclidean domain, for the valuation  $v$  defined by  $v(n) = |n|, n \neq 0 \in \mathbb{Z}.$



(2) If  $F$  is a field, then  $F[x]$  is an Euclidean domain for the valuation  $v$  defined by  $v(f(x)) = \deg[f(x)]$ ,  $f(x) \in F[x]$ ,  $f(x) \neq 0$ .

we find that  $v$  is an Euclidean valuation, where:

(1)  $\forall f(x), g(x) \in F[x] \Rightarrow \deg[f(x)] \leq \deg[f(x)g(x)]$

(2)  $\forall f(x), g(x) \in F[x] \exists q(x), r(x) \in F[x] \Rightarrow$

$f(x) = g(x)q(x) + r(x)$  and  $r(x) = 0$  or  $\deg[r(x)] < \deg[g(x)]$

### III. Theorem (1):

Every Euclidean domain is a principal ideal domain.

□ proof:

Let  $D$  be an Euclidean domain with the Euclidean valuation  $v$ .

Let  $N$  be an ideal in  $D$ .

If  $N = \{0\}$ , then  $N = \langle 0 \rangle \Rightarrow N$  is principal.

If  $N = D$ , then  $N = \langle 1 \rangle \Rightarrow N$  is principal.

~~$N \neq \{0\}$~~

Suppose that  $N \neq \{0\}$ .

Let  $b \in N$   $\exists$   $v(b)$  is minimal among all  $v(n) \forall n \in N$ .

Now, we need to prove that  $N = \langle b \rangle$ .

Let  $a \in N$ .

$\therefore D$  is an Euclidean domain.

$\therefore \exists q, r \in D \exists a = bq + r$ ,  $r = 0$  or  $v(r) < v(b)$ .

$\therefore a = bq + r \Rightarrow r = a - bq$ .



$$\dots a, b \in N$$

$$\therefore a - bq \in N \Rightarrow r \in N$$

$\therefore v(b)$  is chosen to be minimal.

$\therefore v(r) < v(b)$  is impossible.

$$\Rightarrow r = 0.$$

$$\therefore a = bq \Rightarrow N = \langle b \rangle$$

$\therefore N$  is principal.

$\Rightarrow D$  is a principal ideal domain.

#### IV. Corollary :

Every Euclidean domain is a unique factorization domain.

□ proof:

Let  $D$  be an Euclidean domain.

Using the previous theorem which states that "Every Euclidean domain is a principal ideal domain".

$$D - \text{E.D.} \Rightarrow D - \text{P.I.D.} \rightarrow (1)$$

using the theorem which states that "Every principal ideal domain is a unique factorization domain".

$$D - \text{P.I.D.} \Rightarrow D - \text{U.F.D.} \rightarrow (2)$$

From (1) and (2):

$$D - \text{E.D.} \Rightarrow D - \text{U.F.D.} \quad \#$$

⊕ Remark:

not every principal ideal domain is Euclidean domain.



## (2) Arithmetic in Euclidean domains

### I. Theorem (1):

For an Euclidean domain  $D$  with Euclidean valuation  $v$ ,  $v(1)$  is minimal among all  $v(a)$  for nonzero  $a \in D$ , and  $u \in D$  is a unit if and only if  $v(u) = v(1)$ .

□ proof:

Let  $D$  be an Euclidean domain and  $v$  be an Euclidean valuation.

$$\forall a \in D, a = 1 \cdot a.$$

$\therefore D$  is Euclidean domain.

$$\therefore v(1) \leq v(1 \cdot a) = v(a) \quad \forall a \in D.$$

$\Rightarrow v(1)$  is minimal among all  $v(a) \quad \forall a \in D$ .

Now, we need to prove that:

$$u \in D \text{ is a unit} \iff v(u) = v(1).$$

(i) proving that:

$$u \in D \text{ is a unit} \implies v(u) = v(1).$$

Let  $u$  be a unit in  $D$ .

$\therefore v(1)$  is minimal among all  $v(a) \quad \forall a \in D$ .

$$\therefore v(1) \leq v(u). \rightarrow (i)$$

$\therefore u$  is a unit.

$$\therefore \exists u' \in D \ni uu' = 1.$$

$\therefore D$  is an Euclidean domain.

$$\therefore v(u) \leq v(uu') = v(1) \rightarrow (ii)$$



From (i) and (ii) :  $\Rightarrow v(u) = v(1)$ .

(iii) proving that:

$v(u) = v(1) \Rightarrow u \in D$  is a unit.

Let  $v(u) = v(1)$ .

By the division algorithm :

$\exists q, r \in D \ni 1 = uq + r$  where  $r = 0$  or  $v(r) < v(u)$ .

$\therefore v(u) = v(1)$ ,  $v(1)$  is minimal among all  $v(a) \forall a \in D$ .

$\therefore v(r) < v(u)$  is impossible.

$\Rightarrow r = 0$ .

Hence,  $1 = uq \Rightarrow u$  is a unit  $\#$

## II. Definition (1) : (gcd)

Let  $D$  be a U.F.D. An element  $d \in D$  is a greatest common divisor (abbreviated gcd) of elements  $a$  and  $b$  in  $D$ , denoted by  $d = (a, b)$ , if:

- (1)  $d \mid a$  and  $d \mid b$ .
- (2) if  $c \mid a$  and  $c \mid b$ , then  $c \mid d$ .

## III. Definition (2) : (lcm)

Let  $D$  be a U.F.D. An element  $l \in D$  is a least common multiple (abbreviated lcm) of elements  $a$  and  $b$  in  $D$ , denoted by  $l = [a, b]$ , if:

- (1)  $a \mid l$  and  $b \mid l$ .
- (2) if  $a \mid c$  and  $b \mid c$ , then  $l \mid c$ .



#### IV. Theorem (2):

If  $D$  is a (PID) and  $a, b$  are nonzero elements of  $D$ , then there exists a gcd of  $a$  and  $b$ .

Each gcd of  $a$  and  $b$  can be expressed in the form  $\lambda a + \mu b$  for some  $\lambda, \mu \in D$ .

□ proof:

Let  $D$  be a (PID).

Consider the set:

$$N = \{ra + sb \mid r, s \in D\}$$

we need to prove that  $N$  is an ideal of  $D$ .

let  $n_1, n_2 \in N \ni n_1 = r_1a + s_1b, n_2 = r_2a + s_2b$ .

$$n_1 - n_2 = (r_1a + s_1b) - (r_2a + s_2b) = (r_1 - r_2)a + (s_1 - s_2)b \in N$$

$$\therefore n_1 - n_2 \in N \rightarrow (i)$$

let  $k \in D, n \in N \ni n = ra + sb$ .

$$\left. \begin{aligned} kn &= k(ra + sb) = (kr)a + (ks)b \\ nk &= (ra + sb)k = (rk)a + (sk)b \end{aligned} \right\} \rightarrow (ii)$$

from (i) and (ii)  $\Rightarrow N \triangleleft D$ .

$\therefore D$  is a (PID).

$\therefore \exists d \in D \ni N = \langle d \rangle$ .

$\rightarrow ra + sb \in N = \langle d \rangle$ .

$\therefore d \mid ra + sb$

at  $r=1$  and  $s=0 \Rightarrow d \mid a$ .

at  $r=0$  and  $s=1 \Rightarrow d \mid b$ .



$\therefore d|a$  and  $d|b \rightarrow (1)$

Let  $c \in D \ni c|a$  and  $c|b$ .

$\Rightarrow c|ra+sb \quad \forall ra+sb \in N$ .

$\Rightarrow c|n \quad \forall n \in N$

$\therefore d \in N$

$\therefore c|d \rightarrow (2)$

from (1), (2)  $\Rightarrow d = \gcd(a, b)$ .

$\therefore d \in N$

$\therefore \exists \lambda, \mu \in D \ni d = \lambda a + \mu b$

## V. Theorem (3): (Euclidean algorithm)

Let  $D$  be an Euclidean domain with an Euclidean valuation  $v$  and let  $a, b$  be nonzero elements of  $D$ .

let  $r_1 \in D \ni a = bq_1 + r_1$  where,

either  $r_1 = 0$  or  $v(r_1) < v(b)$ .

If  $r_1 \neq 0$ :

let  $r_2 \in D \ni b = r_1 q_2 + r_2$  where,

either  $r_2 = 0$  or  $v(r_2) < v(r_1)$

Continuing in this manner

let  $r_{i+1} \in D \ni r_{i-1} = r_i q_{i+1} + r_{i+1}$  where,

either  $r_{i+1} = 0$  or  $v(r_{i+1}) < v(r_i)$ .

The the sequence  $r_1, r_2, \dots$  must terminate with some

$r_s = 0$ . If  $r_1 = 0$ , then  $b$  is a gcd of  $a$  and  $b$ .

If  $r_1 \neq 0$  and  $r_s$  is the first  $r_i = 0$ , then a gcd of  $a$  and  $b$  is  $(r_{s-1})$



### Example:

Find  $\gcd(22471, 3266)$  in  $\mathbb{Z}$ .

$$a = 22471, b = 3266$$

$$a = b q_1 + r_1 \Rightarrow 22471 = 3266 q_1 + r_1$$

$$\begin{array}{r} 6 \\ 3266 \overline{) 22471} \end{array}$$

$$\Rightarrow 22471 = 3266(6) + 2875$$

$$\therefore q_1 = 6, r_1 = 2875$$

$$\Rightarrow b = r_1 q_2 + r_2 \Rightarrow 3266 = 2875 q_2 + r_2$$

$$\Rightarrow 3266 = 2875(1) + 391$$

$$\therefore q_2 = 1, r_2 = 391$$

$$\Rightarrow r_1 = r_2 q_3 + r_3 \Rightarrow 2875 = 391 q_3 + r_3$$

$$\Rightarrow 2875 = 391(7) + 138$$

$$\therefore q_3 = 7, r_3 = 138$$

$$\Rightarrow r_2 = r_3 q_4 + r_4 \Rightarrow 391 = 138 q_4 + r_4$$

$$\Rightarrow 391 = 138(2) + 115$$

$$\therefore q_4 = 2, r_4 = 115$$

$$\Rightarrow r_3 = r_4 q_5 + r_5 \Rightarrow 138 = 115 q_5 + r_5$$

$$\Rightarrow 138 = 115(1) + 23$$



$$\therefore q_5 = 1, r_5 = 23.$$

$$\Rightarrow \tilde{r}_4 = r_5 q_6 + r_6 \Rightarrow 115 = 23 q_6 + r_6$$

$$\Rightarrow 115 = 23(5) + 0$$

$$\therefore q_6 = 5, r_6 = 0.$$

$$\therefore r_5 = \gcd(a, b)$$

$$\Rightarrow \gcd(22471, 3266) = 23.$$

$$23 = \lambda a + \mu b.$$

$$23 = 138 - 115$$

$$= 138 - (391 - 138(2))$$

$$= 138(3) - 391$$

$$= (2875 - 391(7))(3) - 391$$

$$= 2875(3) - 391(21) - 391$$

$$= 2875(3) - 391(22)$$

$$= 2875(3) - (3266 - 2875)(22)$$

$$= 2875(25) - 3266(22)$$

$$= (22471 - 3266(6))(25) - 3266(22)$$

$$= (25)(22471) - (150)(3266) - (22)(3266)$$

$$= (25)(22471) - (172)(3266)$$

$$= 25a - 172b.$$

$$\therefore \lambda = 25, \mu = -172.$$